ARTIGO PROFISSIONAL DOI 10.52781/cmm.e008

Como a tecnologia está controlando nossa infraestrutura crítica, civis e militares trabalhando juntos para minimizar ciberataques

How technology is controlling our critical infrastructure, civilians and military working together to minimize cyberattacks

Resumo: O objetivo deste documento é analisar a influência do desenvolvimento tecnológico e como esse desenvolvimento aumenta os riscos em nossa infraestrutura crítica. Quando estudamos nosso Estado, olhamos à nossa volta e vemos como a tecnologia está assumindo o controle de todos os nossos sistemas importantes e críticos. Portanto, é necessário encontrar a forma de minimizar os ciberataques através de todas as formas possíveis que nosso Estado possui, tais como as unidades cibernéticas militares, legislações, protocolos de ação, e a parte mais importante: os civis que trabalham em empresas privadas (bancos, hospitais, companhia elétrica e outros). Este trabalho deve fazer isso com dois objetivos principais: primeiro, trabalhando juntos como uma parceria indivisível contra essas ameaças e, segundo, tentando manter os sistemas que formam nossa infraestrutura crítica seguros e protegidos. Para desenvolver este tema, o método descritivo será usado, e a informação é coletada de obras importantes, como a Política Nacional de Estratégia de Segurança Cibernética (Guatemala, Mingob 2018), livros sobre terrorismo ou ciberterrorismo e alguns sites que descrevem o diagnóstico de ciberataques e como essas unidades cibernéticas protegeram sua infraestrutura crítica.

Palavras-chave: Tecnologia. Infraestrutura crítica. Ciberataques.

Abstract: The purpose of this document is to analyze the influence of technological development and how that development increases the risks in our critical infrastructure. When we study our state, we look around and see how technology is taking control of all our important and critical systems. So, It is necessary to find the way of minimizing the cyberattacks through all the possible ways that our state has, such as, the military cyber units, legislation, protocols of act, and the most important part: the civilians that work in private companies (banks, hospitals, the electricity company, and others). This work should do this with two main objectives: first, working together as one indivisible partnership against those threats, and second, trying to maintain the systems that form our critical infrastructure safe and secure. To develop this topic, Will be used the descriptive method, and it is collected the information from important works, such as, The National Cyber Security Strategy Policy (Guatemala, Mingob 2018), books about terrorism or cyber terrorism and some web sites that describe diagnosis of cyber-attacks and how those cyber units have protected their critical infrastructure.

Keywords: Technology. Critical Infrastructure. Cyberattacks.

Aram Albert Jordan Sandoval
Ejército de Guatemala.
Cidade da Guatemala, Guatemala.
jordanaram15@gmail.com

Recebido: 06 de março de 2020
Aprovado: 10 de agosto de 2020

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 Introdução

Desde as últimas duas décadas, a tecnologia tornou-se um eixo transversal no desenvolvimento humano. As pessoas usam tecnologia em seu trabalho diário, ciência, medicina, engenharia e educação, e muitos outros. Tornou-se uma forma fácil de gerenciar todos os nossos serviços ao redor do mundo, banco eletrônico, e-transportation, internet das coisas, e estamos agora muito confortáveis com isso. Essas instalações são a nossa infraestrutura crítica (CARVALHO, 2016). Todos os países do mundo têm uma e talvez a maioria delas estejam interligadas umas com as outras.

Como Paul Shemella em seu livro chamado "Fighting Back" explica algo sobre as motivações de atos terroristas, será parafraseado em palavras compreensíveis como, a maioria dos países do primeiro mundo estão se preocupando em como manter seus sistemas seguros e protegidos. Eles criaram algumas instituições públicas (unidades cibernéticas), que estão lutando para minimizar os ciberataques ou lutando contra os hackers que podem roubar informações críticas, por dinheiro, bens pessoais, ou pior ainda, desestabilizar um país ou um grupo de países que têm relações fortes.

Para iniciar este trabalho, é necessário responder a esta pergunta: Como podem civis e militares trabalhar juntos de forma estratégica para minimizar esses ciberataques? Durante o desenvolvimento deste artigo, é obrigatório encontrar a forma como esses principais atores poderiam trabalhar como uma equipe estratégica para combater as ameaças transnacionais.

Na investigação em um novo mundo tecnológico, será descoberto o significado de infraestrutura crítica, seus componentes, e a importância de manter essas infraestruturas seguras e protegidas, a fim de permitir que os cidadãos tenham sistemas estáveis e fiáveis.

É necessário encontrar uma forma de trabalhar em conjunto (civis e militares) aplicando os padrões internacionais que incluem o monitoramento da infraestrutura 24/7/365, evitando e minimizando ataques e detectando e respondendo a essas ameaças transnacionais (protocolos de ação).

Neste relatório de pesquisa, o leitor irá encontrar informações sobre a terminologia cibernética, a infraestrutura crítica de generalidades e componentes, normas internacionais e nacionais de instituições que foram criadas ou melhoradas, tais como o Grupo de Resposta a Emergências Informáticas (CERTS) [Computer Emergency Response Team] e o Grupo de Resposta a Incidentes de Segurança (CSIRTs) [Computer Security Incident Response Team], (URVIO, 2017), que mostram a maneira ética de monitor, combater e responder aos ciberataques e como eles podem afetar a nossa infraestrutura crítica.

Além disso, esta pesquisa apresenta casos de estudo sobre dois países que estão lutando contra os ciberataques da mesma forma, e ambos estão criando estratégias, leis específicas sobre cibernética, avaliações de risco e uma cultura de consciência em suas sociedades, a fim de proteger a sua soberania e a honra de sua nação. Essa informação será uma fonte de estudo para minimizar os ciberataques e sobre como prevenir e combater esses ciberataques.

No final desta pesquisa, espera-se que civis e militares trabalhem como uma equipe nacional para compartilhar experiências e para que eles tenham uma visão do país sobre ameaças transnacionais como as ameaças cibernéticas. Através da partilha dessas experiências, eles poderiam trabalhar em novas estratégias de defesa nacional.

2 Características gerais

2.1 Ciberdefesa: "A ciberdefesa é um mecanismo de defesa de rede de computadores que inclui respostas a ações e proteção de infraestrutura crítica e garantia de informação para organizações, entidades governamentais e outras redes possíveis. A ciberdefesa se concentra em prevenir, detectar e fornecer respostas oportunas a ataques ou ameaças para que nenhuma infraestrutura ou informação seja adulterada" (CYBER..., 2019, n.p.), defesa de redes de computadores (computer network defense - CND).

2.2 Infraestruturas crítica: "A infraestrutura crítica é o conjunto de sistemas, redes e recursos que são tão essenciais que o seu funcionamento contínuo é necessário para garantir a segurança de uma dada nação, da sua economia e da saúde e/ou segurança do público. Embora a infraestrutura crítica seja semelhante em todas as nações devido aos requisitos básicos da vida, a infraestrutura considerada crítica pode variar de acordo com as necessidades, recursos e nível de desenvolvimento de uma nação" (CRITICAL..., 2019, n.p.).

2.3 Ciberataque: "[...] é a exploração deliberada de sistemas informáticos, empresas e redes dependentes da tecnologia. Os ciberataques usam um código malicioso para alterar código de computador, lógica ou dados, resultando em consequências disruptivas que podem comprometer os dados e levar a cibercrimes, tais como roubo de informações e identidade. [...] [e] também é conhecido como um ataque à rede de computadores (computer network attack - CNA) (CYBERATTACK, 2019, n.p.).

2.4 Grupo de Resposta a Emergências Informáticas (CERT): "[...] é um grupo de especialistas que respondem a incidentes de cibersegurança. Essas equipes lidam com a evolução de malware, vírus e outros ciberataques (COMPUTER..., 2019a, n.p.).

2.5 Grupo de Resposta a Incidentes de Segurança (CSIRT): é uma equipe que responde a incidentes de segurança informática quando eles ocorrem. Um incidente pode ser uma negação de serviço ou a descoberta de acesso não autorizado a um sistema informático (COMPUTER..., 2019b, n.p.).

3 Infraestrutura crítica

3.1 Generalidades

O conceito de infraestrutura começou nos anos 80. Incluía os serviços do setor público, tais como, ferrovias, pontes, aeroportos, transportes públicos, instalações de abastecimento de água e todos os recursos que os estados tinham dentro de seu território. Eles tiveram um papel importante no desenvolvimento de todo o país. Eles forneceram o que a população precisava porque, nessa parte da história, o governo tinha todo o poder do país. No entanto, o conceito mudou nos anos 90 para um conceito de Segurança Nacional, porque os ataques terroristas aumentaram dramaticamente.

A subsistência dos países e o desenvolvimento de sua população incluíam a segurança nacional, não só por causa do significado da palavra, mas também porque eles precisavam fechar as lacunas entre os ataques terroristas e a segurança de sua infraestrutura crítica e estratégica, combinada com informações críticas sobre sua população e a todos os ativos que os estados têm.

Eles são o núcleo de todos os países ao redor do mundo. Então, depois dos acontecimentos do 11 de setembro, o conceito de infraestrutura volta a mudar e, apesar dos fatos, aparece agora incluindo a palavra "crítica" não só para o setor público como nos anos 80, mas para o novo conceito ou a nova forma de falar sobre infraestrutura.

Um dos principais desafios neste conceito é a resiliência, porque esta palavra vai além de seu significado. Inclui a capacidade desses países para dar ao seu povo flexibilidade, adaptabilidade e muitas capacidades de mudança ou redefinir a forma de reagir quando a situação exige esse tipo de resiliência.

Hoje em dia, o conceito de infraestrutura crítica se transforma em um enorme desafio para todos os países ao redor do mundo, devido ao aumento da população, às necessidades de comunicação ou de fazer mais transações bancárias eletrônicas, e a disseminação de tecnologia que poderia tomar uma parte importante na vida humana, e tornou-se um eixo transversal nas rotinas diárias de todos.

Os Estados investirão muito dinheiro em equipamentos modernos, políticas mais severas e mais treinamento para as pessoas que gerirão os novos sistemas que os ajudarão a manter esses três aspectos trabalhando como um todo, a fim de evitar algum phishing de informações ou para evitar algumas intrusões de sistema.

Enquanto isso, todos os serviços nacionais (públicos e privados) funcionariam adequadamente e dariam à sua população todos os materiais e confiança de que necessitam (O'ROURKE, 2007).

3.2 Componentes

Os componentes da Infraestrutura Crítica voltada para o setor público, o setor privado, os sistemas alimentares, os sistemas de defesa industrial, os monumentos nacionais, os bancos, os sistemas financeiros e muitos outros que participam ativamente em todos os países.

Eles são vitais para um país a fim de fornecer à sua população todos os serviços básicos, mantendo o processo de globalização com outros países. Este conceito não é apenas para ciberataques, mas também para desastres naturais, recessões econômicas, falta de serviços vitais, ou países fracos. É necessário proteger e manter seguras e protegidas todas as partes desta infraestrutura, porque se uma delas faltar, o país entrará em colapso a muito curto prazo (O'ROURKE, 2007).

Agora, uma das necessidades mais importantes, é identificar a localização dos nossos recursos estratégicos porque eles representam os ativos mais valiosos do país. Estes recursos estratégicos tornaram-se uma grande parte das infraestruturas críticas e é essencial monitorizar, proteger e identificar onde estão e quão grandes ou úteis são. Devemos adicioná-los ao catálogo da infraestrutura nacional.

4 Padrões internacionais

O Organização Internacional de Normalização (ISO) desempenha um papel importante na cibersegurança e na ciberdefesa por apresentar diretrizes sobre como gerenciar e como conectar segurança e defesa. Refere-se a trabalhar em conjunto, civis e militares. Em seguida, esses países em todo o mundo precisam trabalhar duro como uma equipe nacional, a fim de criar cenários para ajudar e encontrar algumas estratégias nacionais e políticas nacionais para discutir alguns desafios importantes juntos, setores público e privado. Esses padrões tornaram-se ferramentas inestimáveis para compartilhar informações, conhecimentos e experiências que contribuem para manter a infraestrutura crítica segura, e para manter a credibilidade na tecnologia. Desta forma, a população irá usá-los da melhor maneira possível, a fim de dar um espectro muito claro de cibersegurança e ciberdefesa.

As seguintes normas irão apresentar um guia sobre como trabalhar neste novo mundo cibernético.

4.1 ISO 27032

A ISO 27032 apresenta algumas Tecnologias da Informação (TI), sobre técnicas de segurança, a fim de capacitar um Estado sobre cibersegurança, utilizando as técnicas mais importantes e pontos estratégicos relacionados à segurança das redes, segurança da internet e segurança de aplicativos. Esta norma pretende garantir o intercâmbio de informações na rede para que cibercrimes possam ser enfrentados.

A primeira área desta diretriz aborda questões de ciberespaço e cibersegurança, a fim de fechar lacunas em diferentes domínios do ciberespaço e dar uma orientação para abordar os riscos comuns de cibersegurança que incluem ataques de engenharia social, pirataria, malwares, spywares e outros novos softwares maliciosos.

Esse guia de técnicas tem fornecido algumas habilidades sobre como estar preparado para ataques de malware, detecção e rastreamento de ataques, e respostas para esses ataques.

A segunda área focalizada é a mais importante. Chama-se "colaboração" porque é necessário ser eficaz e eficiente para compartilhar e trocar informações e coordenar como os incidentes serão geridos. Esta colaboração será segura e confiável, a fim de proteger as informações das partes interessadas. A norma inclui a integração e interoperabilidade do sistema em ambos os sentidos (JUMBO VIVANCO, 2019).

4.2 ISO 31000

A ISO 31000, de acordo com (PALACIOS GUILLEM; GISBERT SOLER; PÉREZ BERNABEU, 2015) descreve, de forma compreensível, o significado de gestão de riscos. Por conseguinte, neste caso, é muito importante aproveitar o planejamento ou o processo de tomada de decisão, porque esses Estados devem estar cientes dos ciberataques, das catástrofes naturais ou de qualquer ataque que desestabilize os países.

É necessário fazer algumas avaliações de risco sobre a nossa infraestrutura crítica, sem qualquer restrição, mas de uma maneira paralela, é urgente ter um plano que atribui responsabilidades para todos os diferentes setores incluídos e fornecer-lhes possíveis maneiras para prevenir, mitigar, e recuperar diferentes tipos de ataque. Também é importante dar-lhes a oportunidade de trabalhar na mesma equipe, militares e civis, a fim de proteger a infraestrutura e atender os riscos juntos, tentando minimizar os danos, especialmente se trata-se de um ciberataque, porque o dano poderia ser imediato e calamitoso. As consequências seriam piores, por exemplo, se o ciberataque bloqueia o aprovisionamento energético ou o setor bancário ou faz com que as infraestruturas críticas colapsem.

4.3 ISO 27005

Quando um dos principais objetivos é proteger a infraestrutura crítica, refere-se à gestão dos riscos para a segurança da informação que a ISO 27005 apresenta. Ela tem sido um quadro de referência sobre a metodologia entre a gestão do risco e a segurança da informação, e fornece cinco etapas importantes:

a) O plano interior e exterior
b) A definição do contexto organizacional (interior e exterior)
c) A valorização dos riscos tecnológicos
d) O tratamento dos riscos tecnológicos
e) Acompanhamento e um processo contínuo de gestão do desenvolvimento

Em primeiro lugar, um plano de comunicação que seria difundido no interior e no exterior da infraestrutura crítica do setor público e privado, e através deste plano, determinar os riscos e objetivos a fim de apresentar um resumo sobre os avanços no processo. A melhor maneira de divulgar essa informação seria utilizando material escrito e treinando pessoas sobre esses aspectos.

Por outro lado, este plano de comunicação seria elaborado a fim de criar consciência e segurança, e o mais importante, para evidenciar a existência de riscos.

Este plano teria três aspectos diferentes a considerar: a comunicação primária, que inclui conceitos gerais, implicações e vantagens. A seguir, comunicação no caminho. Este aspecto apresenta avanços na gestão de riscos, a fim de ter feedback e apoio das pessoas que estão trabalhando no risco. E por último, comunicações de resultados que tentarão compartilhar e difundir as informações alcançadas por meio deste plano.

A segunda etapa da gestão de risco é um contexto organizacional que integra missão, visão, políticas, estratégias, papéis e responsabilidades. A importância deste contexto é a ordem em que a infraestrutura crítica será protegida quando um ciberataque vier, e encontrar as limitações para proteger todos os sistemas de informação, e como uma equipe de resposta nacional aceitaria o nível de risco e, desta forma, eles determinariam os alcances e limitações que a infraestrutura crítica possui.

O terceiro aspecto é a valorização do risco tecnológico. Nesta fase, os ativos nacionais de informação poderiam ser identificados e, desta forma, poderia determinar qual é o

mais importante a ser protegido. Também pode estabelecer as ameaças às quais a infraestrutura crítica está sendo exposta para mitigar os riscos. Esta valorização pode ser sobre aquisição de custos, renovação, recuperação ou manutenção. Por outro lado, é necessário identificar as ameaças de infraestrutura crítica que poderiam ser físicas, lógicas ou estratégicas, e de acordo com sua origem: naturais, técnicas, acidentais ou intencionais. Isso ajudaria a identificar os riscos dessas ameaças e a determinar o impacto em todas as partes interessadas.

O quarto aspecto é a maneira de lidar com os riscos tecnológicos, porque nesta fase, é necessária uma avaliação dos danos, a fim de mitigar os riscos e danos colaterais. Essa ação poderia ser usada para reduzir, aceitar e eliminar danos.

Este plano precisa definir políticas e diretrizes e criar uma unidade de comando e controle para realizar as tarefas de recuperação e levar a infraestrutura crítica ao seu estado normal. Desta forma, todos os serviços e a confiança seriam devolvidos às partes interessadas.

E finalmente, a melhoria contínua. Com isso, podem ser criados controles de mudança de ativos, processos, vulnerabilidades, ameaças e políticas com o objetivo de estabelecer as seguintes ações e manter a gestão atualizada, a fim de avaliar indicadores de acordo com os que aparecem em planos exteriores ou interiores (RAMIREZ CASTRO; ORTIZ BAYONA, 2011).

5 Protegendo a infraestrutura crítica - casos de estudo: República Federativa do Brasil e República da Guatemala

5.1 Estratégia Nacional de Cibersegurança da Guatemala

Falando sobre a Guatemala, em 2018, o Ministério do Interior publicou a Estratégia Nacional de Cibersegurança, a fim de fornecer as diretrizes das instituições governamentais sobre um tema que só o Ministério da Defesa e o Ministério do Interior abordaram. É necessário informar ao restante do Estado sobre os temas em alta da segurança nacional, a fim de criar consciência social e a responsabilidade que essas instituições têm como servidores públicos. É também importante informar a população guatemalteca sobre as questões de segurança nacional que eles precisam combater e como lidar com elas.

A estratégia nacional de cibersegurança, como é mencionado no resumo desta pesquisa (GUATEMALA, 2018), inclui:

a) Infraestrutura crítica
b) Tecnologias de informação e comunicação
c) Pesquisa e resposta a incidentes cibernéticos
d) Quadros legais
e) Governança
f) Missão, visão, objetivos e outros

Em primeiro lugar, esta nova estratégia refere-se à Organização dos Estados Americanos (OEA) em sua resolução AG/RES 2004 "*Adoção de uma Estratégia Global Interamericana de Combate às Ameaças à Cibersegurança: Uma Abordagem Multidimensional e Multidisciplinar para a Criação de uma Cultura de Cibersegurança*". Essa resolução é a ponta de lança do modelo guatemalteco de estratégia de cibersegurança. Essa estratégia diz literalmente nos seus cinco primeiros pontos de resolução:

> 1. Adotar a Estratégia Global Interamericana de Cibersegurança: Uma Abordagem Multidimensional e Multidisciplinar para a Criação de uma Cultura de Cibersegurança, em anexo como Apêndice A.
> 2. Instar os Estados-Membros a aplicarem a referida Estratégia.
> 3. Instar os Estados-Membros a criarem ou identificarem grupos nacionais de "alerta, vigilância e aviso", também conhecidos por "Grupos de Resposta a Incidentes de Segurança" (CSIRTs).
> 4. Colocar ênfase renovada na importância de alcançar sistemas de informação seguros na Internet em todo o Hemisfério.
> 5. Solicitar que o Conselho Permanente, por intermédio da Comissão de Segurança Hemisférica, continue a resolver esse problema e a facilitar a coordenação de esforços para a implementação da Estratégia, em especial os esforços de especialistas do governo, o Comitê Interamericano Contra o Terrorismo (CICTE), a Comissão Interamericana de Telecomunicações (CITEL), o Grupo de Peritos Governamentais em Matéria de Delito Cibernético da Reunião de Ministros da Justiça ou de Ministros ou Procuradores-Gerais das Américas (REMJA), e outros órgãos da OEA (ORGANIZATION OF AMERICAN STATES, 2004, n. p., ênfase acrescentada).

Esta resolução da OEA fornece as diretrizes sobre como a América Latina está enfrentando as questões de cibersegurança com uma perspectiva multidimensional e multidisciplinar, a fim de criar uma cultura cibernética nos países que fazem parte dela. Esta organização está incentivando os países latinos a implementar esta estratégia como sua estratégia nacional, a fim de criar padrões regionais de cibersegurança. Esses países têm a sua própria maneira de detectar, prevenir e responder a qualquer ciberataque, mas não têm uma estratégia comum que os permita trabalhar em conjunto de uma forma multidimensional. A OEA incentiva esses países a estabelecer e identificar Grupos de Resposta a Emergências Informáticas (CERTs) e Grupos de Resposta a Incidentes de Segurança (CSIRTs), a fim de integrar todas essas equipes nacionais, regionais e internacionais como uma grande equipe. Essas equipes terão um relacionamento confiável especial na forma de compartilhar informações vitais contra um ciberataque. Finalmente, o Comitê Interamericano Contra o Terrorismo (CICTE) trabalhará como coordenador para esta estratégia, enquanto os outros departamentos da OEA participarão da estratégia quando necessário.

Esta estratégia é da maior importância para o modelo guatemalteco de cibersegurança, porque as ameaças transnacionais e os ciberataques evoluem, e as atividades eletrôni-

cas diárias participam da zona digital, e os sistemas nacionais estão interligados. Será necessário ter uma estratégia que proporcione a todos os setores guatemaltecos a oportunidade de criar quadros técnicos e quadros legais para fortalecer a cibersegurança nacional e global. Esta estratégia apresenta um componente importante com um grande valor, a resiliência. Será necessária para redefinir o mais rapidamente possível todos os serviços, evitando com esta recuperação, a perda de informações e danos colaterais, a fim de proteger o ativo mais valioso do país, sua população.

Esta estratégia foi criada no início de um processo que envolveu mais de uma centena de fatores chave nacionais e regionais dos diferentes setores da sociedade guatemalteca (militares e civis) de acordo com o plano estratégico de segurança nacional (2016-2020), a agenda de riscos e ameaças nacionais, e a agenda de segurança estratégica da nação. Esta estratégia analisa o cenário que a Guatemala precisa para mitigar os riscos e ameaças que vêm do ciberespaço.

Os objetivos que esta estratégia mostra são orientados para fortalecer as capacidades e os protocolos de ação das instituições que fazem parte do sistema nacional de segurança na Guatemala, atribuindo-lhes responsabilidades para agir com base em um quadro legal, a fim de manter o estado de direito na Guatemala.

A Guatemala está envolvida em marcos internacionais que regulam a cooperação em termos de infraestruturas críticas, e, claro, eles são liderados pelos Estados Unidos, que é o primeiro país a criar um documento relacionado à proteção da infraestrutura crítica. Este documento explica a necessidade de criar um comitê. Este comitê avaliaria as vulnerabilidades dos ataques terroristas, a fim de proteger essa infraestrutura numa dimensão transnacional. A Guatemala tem muitas infraestruturas públicas e outras do setor privado, mas não tem como articular todas elas e como trabalhar com as melhores práticas em procedimentos de segurança da informação.

Como corolário dessa estratégia, a Guatemala criou duas coisas depois de publicar isso. A primeira foi um comitê técnico que inclui o setor governamental, o setor privado, as academias, as infraestruturas críticas, o setor financeiro e o setor de TI, a fim de reforçar as relações de colaboração, cooperação e coordenação entre eles, promovendo análises e iniciativas que aumentem o ecossistema de cibersegurança na Guatemala.

A segunda, de acordo com o acordo governamental guatemalteco 65-2019, o Comando Informático e Tecnológico foi criado pelo Ministério da Defesa. Este comando é responsável pela coordenação de todos os temas de ciberdefesa, trabalhando com instituições nacionais e internacionais que gerenciam esses temas e se tornando parte desse esforço nacional e internacional.

5.2 As ameaças cibernéticas brasileiras

Em 2005, depois de muito tempo sem uma política de defesa no Brasil, o governo brasileiro emitiu um Plano Nacional de Defesa (PND). O principal objetivo deste plano é criar uma consciência para todos os setores do país, a fim de defender a nação, e estabelecer a importância estratégica do setor cibernético. Esse setor deveria ser mais forte porque o

Brasil tem muitos sistemas com vulnerabilidades e eles precisam criar mais capacidades para evitar essas vulnerabilidades e para recuperar, o mais rápido possível, todas as suas TICs (tecnologias de informação e comunicação). Esse plano inclui todas as ações de segurança da infraestrutura crítica e aplica todos os dispositivos e procedimentos que ajudam a reduzir ou minimizar vulnerabilidades quando afetam seus sistemas de defesa nacional de ciberataques. Há instituições encarregadas deste importante desafio. Essas instituições são: a Casa Civil ou a Presidência, o Ministério da Defesa, o Ministério das Comunicações, o Ministério da Ciência e Tecnologia e o Gabinete de Segurança Institucional (AMARAL, 2014).

A informação anterior é uma prova de que o governo brasileiro está trabalhando com civis e militares, através de sua política estratégica nacional, para proteger os sistemas de defesa dos ciberataques, e esse trabalho inclui a proteção de sua infraestrutura crítica.

O plano está colocando todos os setores nacionais na mesma direção, sejam eles setores privados ou públicos, e eles gerarão mais capacidades para ganhar muito conhecimento cibernético. Eles estão sendo treinados para prevenir, proteger e responder a qualquer ameaça nacional ou internacional que possa levar o Brasil a uma situação crítica que possa causar a perda de sua hegemonia e liderança em cibersegurança e ciberdefesa na América do Sul.

O Gabinete de Segurança Institucional desenvolveu em 2010 o Livro Verde de Segurança Cibernética, com o objetivo principal de criar um ambiente de cibersegurança para proteger a sociedade brasileira e a nação. Este livro verde foi feito para enfrentar os novos desafios e agendas mútuas nos setores privado, público, academias e o "terceiro setor" referindo-se às instituições privadas, mas não lucrativas de acordo com (what is the third sector) (¿QUE ES..., 2018).

É um esforço conjunto de civis e militares para criar um pensamento comum e construir junto as diretrizes da cibersegurança com esses vetores: político-estratégico, econômico, meio ambiente, comunicações, tecnologia, educação, quadro legal, cooperação internacional, transporte, abastecimento de água, financiamento e abastecimento de energia, e quando localizados esses vetores no mesmo pote, eles criam sua infraestrutura crítica.

A coisa mais importante para o setor cibernético foi atribuir essa enorme responsabilidade a uma força armada através do Ministério da Defesa, e depois disso, eles criaram um comando de ciberdefesa. Essa unidade tem a missão de contribuir para aumentar o nível de cibersegurança. Esta unidade cibernética tem o conhecimento para trabalhar com diferentes setores e com a sociedade brasileira. Essa unidade militar está tentando se concentrar na criação de recursos humanos, doutrina e aplicação da segurança com o objetivo de oferecer à população uma resposta rápida a incidentes, lições aprendidas e proteção contra ciberataques (AMARAL, 2014).

Em 2012, o Ministério da Defesa publicou um documento que continha uma nova política de ciberdefesa. Ela estabeleceu a forma de gerir um sistema de ciberdefesa militar. Este documento foi escrito para definir as tarefas da força armada a fim de impedir a internet e outras redes do uso criminoso, e para proteger todos os dados de informação e as comunicações essenciais. Com esta política, o exército brasileiro foi capacitado e assumiu todo o controle cibernético em todo o país. Esse controle inclui a responsabilidade de reunir com todos os setores atribuindo-lhes suas próprias responsabilidades neste tema de segurança nacional.

Ele também incluiu instruções sobre como compartilhar informações, protocolos de ação e a maneira imediata de responder em caso de um ciberataque, construindo com esse controle, relações confiáveis entre esses setores e o exército, a fim de dar o primeiro alerta nacional e fazer com que o plano de cibersegurança continue.

Imediatamente depois de um ciberataque, uma equipe nacional de resposta entrará em contato com todos os seus membros para fornecer informações específicas do campo, a fim de encontrá-los assim que possível, dependendo do tipo de ciberataque, local dos eventos, principais danos e determinar quais poderiam ser as primeiras decisões a tomar. Um dos principais desafios é mitigar os danos e tentar resolver o problema imediatamente. Com essa reação, a unidade de ciberdefesa coordenará com outras instituições que têm a responsabilidade de investigar e criminalizar este ataque de acordo com seu quadro legal.

Esta breve descrição explica as primeiras ações contra um ciberataque, como ativar o plano de cibersegurança, e a maneira de criminalizar o cibercrime se ele existir, ou se este ataque faz parte de uma questão de ciberterrorismo, a fim de alertar os países vizinhos brasileiros ou países ao redor do mundo.

Hoje em dia, o Brasil tem um passo à frente em comparação com seus vizinhos. Está muito perto de consolidar seu sistema de cibersegurança e ciberdefesa do mais alto nível político, com cobertura nacional, representada pelo Gabinete de Segurança Nacional, pela Administração Pública Federal e pelo Ministério da Defesa, que constrói a ligação política-estratégica, aos níveis mais baixos das unidades do exército. Essas unidades trabalham em níveis operacionais e táticos no sistema de cibersegurança e ciberdefesa, incluindo nesse nível os civis que trabalham em níveis médio e baixo em todos os tipos de setores, a fim de defender seus interesses cibernéticos nacionais.

No sistema de cibersegurança e ciberdefesa, o Gabinete mencionado no último parágrafo tem a tarefa de coordenar todas as ações que afetam a sociedade, por exemplo, as questões de cibersegurança, informação e comunicação, e a segurança nacional de infraestrutura crítica.

O Ministério da Defesa supervisiona todas as questões relacionadas à ciberdefesa e recebeu as seguintes ordens:

a) Nível Estratégico: O Ministério da Defesa será responsável pela criação de protocolos que os permitam fazer parte do quadro legal de acordo com suas leis nacionais e seus acordos internacionais de ações que os envolvam em situações de crise ou conflitos armados e operações de manutenção da paz.

b) Nível Operacional: Aqui, o Ministério da Defesa, como todos os exércitos de todo o mundo, deve estar preparado para conduzir operações militares defensivas ou ofensivas, a fim de preservar a sua soberania e a honra da nação. Neste conceito, o Exército Brasileiro também inclui todos os problemas que afetam seu ambiente cibernético (AMARAL, 2014).

Com essa importante política, o Ministério da Defesa e o Exército Brasileiro estão assumindo o controle de todas as infraestruturas críticas em todo o país. Eles são a ligação entre as instituições nacionais e as empresas privadas que estão interligadas e trocando

informações classificadas das pessoas que vivem no Brasil ou das pessoas que estão fazendo transações eletrônicas, dentro ou fora das fronteiras brasileiras. Eles esperam que o governo brasileiro lhes forneça um alto nível de segurança de suas informações pessoais para não ser um objetivo para um ciberataque, ou para obter suas informações roubadas (phishing), ou para serem vítimas de extorsão do crime organizado.

O nível de segurança deve ser oferecido a essas pessoas, a fim de aumentar os investidores estrangeiros e tornar o ambiente empresarial mais fiável. Desta forma, o comércio internacional brasileiro será mais confiável.

Por outro lado, o governo brasileiro tem uma infraestrutura crítica mais forte para conservar seus recursos naturais em lugares seguros e também protege suas áreas estratégicas.

Hoje em dia, essas áreas estratégicas estão sendo afetadas pelo crime organizado e ameaças transnacionais que precisam ter essas áreas para aumentar sua riqueza.

É por isso que a equipe de segurança nacional e a equipe de defesa nacional, combinando os seus recursos e capacidades, precisam trabalhar juntas para se tornarem mais poderosas, e desta forma, elas vão detectar, prevenir e responder a todos os atos que possam afetar a sua infraestrutura crítica nacional e os sistemas que gerenciam essa infraestrutura.

6 Conclusões

A fim de tirar conclusões, é obrigatório considerar como a tecnologia está se tornando uma parte importante da vida das pessoas em todo o mundo. A tecnologia aumentou mais de 50% de todas as descobertas durante o século passado. Ela ajuda em todas as atividades diárias como um eixo transversal na ciência, tarefas domésticas, ações militares e muitas outras que incluem a infraestrutura crítica em todos os países.

Os seres humanos encontraram um conjunto de coisas que tornaram suas atividades e até suas vidas mais fáceis, a fim de ganhar mais tempo para fazer outras atividades. É por isso que essas atividades são o escopo desta pesquisa porque precisam de uma maneira de fornecer mais ferramentas tecnológicas para as pessoas em todo o mundo. Os desenvolvedores de software e hardware ou as empresas que geriram sistemas não perceberam como essas descobertas eram perigosas não só por causa das ferramentas, mas também por causa da forma como as pessoas usam essas ferramentas.

O desenvolvimento tecnológico deve continuar, além dele, um grande componente de segurança, a fim de fornecer conexões confiáveis e manter o nível de segurança nacional no topo em todos os países e segurança coletiva em sua região.

Depois de dizer isso, é necessário referir-se aos governos que criaram muitas instituições que têm a responsabilidade de estabelecer diretrizes para fornecer cibersegurança para questões internas, e equipes de ciberdefesa para resolver questões internas, externas, regionais e continentais. Essas instituições estão combinando seus melhores esforços para trabalhar em conjunto, civis e militares, e agora o novo desafio é trabalhar com muitas agências diferentes não só para compartilhar informações, mas para construir uma estratégia comum para combater e minimizar os ciberataques também. Esses ataques podem afetar a

estabilidade de todo o país e, portanto, a estabilidade de qualquer região, pois a maioria de seus sistemas estão interligados para fornecer serviços de e-banking, operações financeiras, fornecimento de luz de energia, e muitos outros, por exemplo, que devem ser garantidos através de um nível de segurança nacional, e como uma parte do governo, isso deve ser feito dentro do país.

Além disso, é necessário falar sobre equipes de segurança nacional que desempenham um papel importante neste tema de segurança, porque o Grupo de Resposta a Emergências Informáticas e o Grupo de Resposta a Incidentes de Segurança são ferramentas estratégicas para os governos. Eles são a primeira linha de defesa quando um ciberataque ocorre. Esses grupos têm a capacidade de lutar contra um ataque ou ataques a fim de prevenir, combater e responder a tarefas para as quais são treinados.

Esses grupos trabalham em conjunto nos setores público e privado. Aproveitando sua experiência, eles irão mitigar os danos colaterais após um ataque em qualquer área de infraestrutura crítica, e eles têm a responsabilidade de parar o ataque, e também a responsabilidade de levar as coisas a um estado normal em um período mínimo de tempo. Esses foram os objetivos mais importantes quando esses grupos foram criados.

Por outro lado, os grupos que estão criando normas internacionais devem ser tidas em conta para seguir as regras de avaliação de riscos que constituem uma parte importante deste instrumento, porque, antes dessas avaliações de risco, esses governos não sabiam quais eram as suas ameaças, ou como era constituída a infraestrutura crítica, ou qual era o seu nível de segurança nacional. Depois de ter avaliações de risco, as normas internacionais dão-lhes uma orientação precisa para fazer um plano estratégico sobre como prevenir, combater e responder a um ciberataque, e como recuperar a estabilidade depois disso.

Quando se fala de infraestruturas críticas, os seus componentes não podem ser eliminados. Esses componentes são a razão da nação e de seus participantes, pois eles não têm risco separadamente, mas quando trabalham juntos, como uma engrenagem em um país, eles se tornam uma importante infraestrutura que precisa ser protegida para fornecer em primeiro lugar a confiança para as pessoas e também confiança para uma região a fim de investir e aumentar transações tecnológicas no comércio, finanças, banking, e outros aspectos. Como demonstrado no corpo desta pesquisa, cada país possui a sua própria infraestrutura crítica, mas em algum momento, esses países precisam estar interligados com os sistemas de outros países e, dessa forma, passa a ser uma meta a ser protegida pela segurança coletiva.

É importante dizer que é necessário rever periodicamente o plano de infraestrutura crítica para que o nível político-estratégico no país mantenha o controle sobre quais instituições foram criadas, e verificar se precisam entrar em sua infraestrutura crítica e, desta forma, eles podem manter seu plano de avaliação de risco atualizado.

Para seguir a ordem lógica nesta pesquisa, foram incluídos dois países que têm quase as mesmas questões e os mesmos esforços para lutar contra os ciberataques. Esses países são a República da Guatemala e a República Federativa do Brasil. Cada um deles tem problemas, mas está assumindo a difícil tarefa de trabalhar em conjunto, civis e militares, setores privado e público, como uma equipe contra os problemas que eles precisam combater. Eles

estão trabalhando juntos em um trabalho de interagências, a fim de minimizar os ciberataques protegendo sua infraestrutura crítica.

No final desta pesquisa, é necessário destacar a necessidade de os países fornecerem uma estratégia especial para trabalhar juntos contra as ameaças cibernéticas, mas também é necessário criar uma cultura de consciência em todas as sociedades, porque as pessoas são os olhos da nação nas ruas e nas redes sociais. Uma vez que as pessoas e as redes sociais estão em contato todos os dias, elas poderiam fornecer informações importantes para alimentar os sistemas de inteligência nacionais. Todos os países devem investigar profundamente as pessoas que gerenciam os sistemas de infraestrutura crítica, a fim de ter equipes com um alto nível de confidencialidade, honestidade e transparência.

Referências

AMARAL, A. C. La amenaza cibernética para la seguridad y defensa de Brasil. **Revista Visión Conjunta**, Buenos Aires, n. 10, p. 19-22, 2014. Disponível em: http://cefadigital.edu.ar/bitstream/1847939/32/3/VC%2010-2014%20AMARAL.pdf. Acesso em: 19 de abril de 2020.

CARVALHO, P. S. M. de. A defesa cibernética e as infraestruturas críticas nacionais. In: EXÉRCITO. Comando Militar do Sul. Núcleo de Estudos Estratégicos. **Biblioteca do NEE**. Porto Alegre: Núcleo de Estudos Estratégicos, 2016. Disponível em: http://www.nee.cms.eb.mil.br/attachments/article/101/cibernetica.pdf. Acesso em: 19 de abril de 2020.

COMPUTER emergency response team (CERT). *In*: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019a. Disponível em: https://www.techopedia.com/definition/31003/computer-emergency-response-team-cert. Acesso em: 10 de novembro de 2019.

COMPUTER security incident response team (CSIRT). *In*: TECHNOPEDIA. Dictionary. Cybersecurity. Edmonton: Techopedia Inc., 2019b. Disponível em: https://www.techopedia.com/definition/24837/computer-security-incident- response-team-csirt. Acesso em: 10 de novembro de 2019.

CYBER defense. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Disponível em: https://www.techopedia.com/definition/6705/cyber-defense. Acesso em: 10 de novembro de 2019.

CYBERATTACK. In: TECHNOPEDIA. Dictionary. **Cybersecurity**. Edmonton: Techopedia Inc., 2019. Disponível em: https://www.techopedia.com/definition/24748/cyberattack. Acesso em: 10 de novembro de 2019.

Infraestrutura crítica. In: WHATLS.COM. Newton, MA: Tech Target, 2019. Disponível em: https://whatis.techtarget.com/definition/critical-infrastructure. Acesso em: 10 de novembro de 2019.

GUATEMALA. Ministerio de Gobernación. **Estrategia nacional de seguridad cibernética**. Guatemala de la Asunción: Ministerio de Gobernación, mar 2018. E-book. (Documento técnico, n. 1). Disponível em: https://uip.mingob.gob.gt/wp-content/uploads/2019/03/Estrategia-Nacional-de-Seguridad-Cibern%C3%A9tica.pdf. Acesso em: 19 de abril de 2020.

JUMBO VIVANCO, P. L. **Implementación de un siem para el comando de ciberdefensa utilizando herramientas de código abierto bajo el estándar ISO 27032**. 2019. Thesis (Ingeniero en Sistemas Informáticos) – Universidad Tecnlógica Israel, Quito, Ecuador, 2019. Disponível em: http://repositorio.uisrael.edu.ec/bitstream/47000/2000/1/UISRAEL-EC-SIS-378.242-2019-033.pdf. Acesso em: 19 de abril de 2020.

O'ROURKE, T. D. Critical infrastructure, interdependencies, and resilience. **The Bridge**, Washington, DC, v. 37, n. 1, p. 22-29, 2007.

ORGANIZATION OF AMERICAN STATES. The General Assembly. **AG/RES 2004 (XXXIV-O/04)**: Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity. [Washington, DC]: June 8, 2004. (Adopted at the fourth plenary session held on June 8, 2004). Disponível em:: https://2009-2017.state.gov/p/wha/rls/59284.htm. Acesso em: 22 de abril de 2020.

PALACIOS GUILLEM, M.; GISBERT SOLER, V.; PÉREZ BERNABEU, E. Sistemas de gestión de la calidad: lean manufacturing, kaizen, gestión de riesgos (UNE-ISO 31000) e ISO 9001. **3C Tecnología**: Glosas de Innovación Aplicadas a La Pyme, [Alicante], v. 4, n. 4, p. 175-188, 2015. Disponível em: https://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/324. Acesso em: 22 de abril de 2020.

¿QUE ES el tercer sector?. In: AYUDA EN ACCION, Madrid, 7 feb 2018. Disponível em: https://ayudaenaccion.org/ong/blog/solidaridad/que-es-el-tercer-sector/. Acesso em: 19 de novembro de 2019.

SHEMELLA, P. (ed.). **Fighting back**: what government can do about terrorism. California: Stanford University Press, 2011.

RAMIREZ CASTRO, A.; ORTIZ BAYONA, Z. Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. **Ingeniería**, Bogotá, v. 16, n. 2, p. 56-66, Jul/Dic 2011. Disponível em: https://revistas.udistrital.edu.co/index.php/reving/article/view/3833. Acesso em: 26 de abril de 2021.

URVIO: Revista Latinoamericana de Estudios de Seguridad. Quito, Ecuador: FLACSO, n. 20, jun./nov. 2017. Disponível em: https://revistas.flacsoandes.edu.ec/urvio/issue/view/150. Acesso em: 19 de abril de 2020.