CEBRI

CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

NÚCLEO
SEGURANÇA
INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA
CIBERNÉTICA (GRUPO CYBER)

OS CONSTANTES DESAFIOS EM **SEGURANÇA CIBERNÉTICA** NAS ORGANIZAÇÕES COMO PARTE DA ESTRATÉGIA DOS NEGÓCIOS

PENSAR
DIALOGAR
DISSEMINAR
INFLUENCIAR

#2 *Think tank* da
América do Sul e Central

University of Pennsylvania's Think Tanks and Civil Societies Program 2019 Global Go To Think Tank Index Report

---

O Centro Brasileiro de Relações Internacionais (CEBRI) é um *think tank* independente, que contribui para a construção da agenda internacional do Brasil. Há mais de vinte anos, a instituição se dedica à promoção do debate plural e propositivo sobre o cenário internacional e a política externa brasileira.

O CEBRI prioriza em seus trabalhos temáticas de maior potencial para alavancar a inserção internacional do país à economia global, propondo soluções pragmáticas na formulação de políticas públicas.

É uma instituição sem fins lucrativos, com sede no Rio de Janeiro e reconhecida internacionalmente. Hoje, reúne cerca de 100 associados, que representam múltiplos interesses e segmentos econômicos e mobiliza uma rede de profissionais e organizações no mundo todo. Além disso, conta com um Conselho Curador atuante e formado por figuras proeminentes na sociedade brasileira.

www.cebri.org

Rua Marquês de São Vicente, 336 – Gávea – Rio de Janeiro / RJ - CEP: 22451-044
Tel + 55 21 2206-4400 - cebri@cebri.org.br - www.cebri.org

CEBRI
CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

NÚCLEO
SEGURANÇA
INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA
CIBERNÉTICA (GRUPO CYBER)

1º WEBINAR DO GRUPO CYBER
25 DE AGOSTO DE 2020

OS CONSTANTES DESAFIOS EM **SEGURANÇA CIBERNÉTICA** NAS ORGANIZAÇÕES COMO PARTE DA ESTRATÉGIA DOS NEGÓCIOS

Paulo Sergio Melo de Carvalho
Senior fellow do CEBRI e General de Divisão da
Reserva do Exército Brasileiro

PARCERIA: SIEMENS SIEMENS energy

FICHA TÉCNICA

AUTOR

Paulo Sergio Melo de Carvalho

Senior Fellow do Núcleo Segurança Internacional do CEBRI
e General de Divisão da Reserva do Exército Brasileiro

COORDENAÇÃO EDITORIAL

Julia Dias Leite
Diretora-Presidente do CEBRI

Luciana Gama Muniz
Diretora de Projetos do CEBRI

Cintia Hoskinson
Consultora de Projetos do CEBRI

APOIO EDITORIAL

Wilma Rodrigues D´Oliveira Kroff

DIAGRAMAÇÃO

Presto Design

NÚCLEO SEGURANÇA INTERNACIONAL

GRUPO DE ANÁLISE DE SEGURANÇA CIBERNÉTICA

O Núcleo Segurança Internacional possui como objetivo principal engajar os setores público e privado, a academia e a sociedade civil em um debate plural sobre temas de segurança internacional e defesa através da produção de publicações e da promoção de debates abertos, *webinars* e debates fechados em formato Chatham House.

O Grupo de Análise de Segurança Cibernética (Grupo Cyber) é desenvolvido no âmbito do Núcleo Segurança Internacional e tem como foco discutir e aprofundar o conhecimento sobre temas estratégicos e contemporâneos relacionados às questões de cibersegurança, tais como: o alinhamento de diferentes abordagens de governança cibernética e resiliência cibernética; regulação e prevenção de conflitos no espaço cibernético; a importância da rede 5G e os riscos relacionados à tecnologia; o impacto do 5G na economia brasileira e na competitividade das indústrias no Brasil; 5G como elemento propulsor da inserção internacional do Brasil no cenário digital global; a crescente migração do multilateralismo para o espaço cibernético e oportunidade para atuação da ONU nesse âmbito.

CONSELHEIRO

André Clark

André Clark é General Manager da Siemens Energy Brasil, tendo sido anteriormente Presidente e CEO da Siemens no Brasil e também CEO da ACCIONA para o Brasil, Bolívia, Uruguai e Paraguai. É formado em Engenharia Química pela Universidade de São Paulo (USP) e possui MBA em Finanças e Gestão de Operações pela Stern School of Business, da Universidade de Nova Iorque. Além disso, hoje também é: Vice-presidente do Conselho Administrativo e Coordenador do Comitê da Indústria da Associação Brasileira de Infraestrutura e Indústrias de Base (ABDIB); Vice-presidente da Diretoria Plenária da Associação Brasileira de Máquinas e Equipamentos (ABIMAQ); Membro do Conselho Empresarial do grupo formado por Brasil, Rússia, Índia, China e África do Sul (BRICS); Membro do Comitê de Líderes da Confederação Nacional da Indústria e do Comitê de Líderes da Mobilização Empresarial pela Inovação (CNI/MEI); Membro do Conselho Curador e coordenador do Núcleo Infraestrutura e do Núcleo Segurança Internacional (CEBRI); Membro do Conselho Consultivo do GRI Club Brasil; Membro do Conselho Superior da Câmara Internacional do Comércio (ICC); Membro da Diretoria e Presidente do Conselho de Transformação Digital do Instituto Brasileiro de Petróleo, Gás e Biocombustíveis (IBP); e Diretor do Conselho Empresarial Brasil-China (CEBC).

SENIOR FELLOW

Paulo Sergio Melo de Carvalho

General de Divisão da Reserva do Exército Brasileiro, especialista em Tecnologia da Informação e Comunicações, com atuação na área de Cibernética nos níveis político-estratégico e operacional-técnico, tendo chefiado o Centro de Defesa Cibernética, de 2014 a 2016, e sendo o primeiro comandante do Comando de Defesa Cibernética, criado em 2016. Atualmente, presta consultoria no setor cibernético e participa na capacitação de recursos humanos, no Brasil e no exterior.

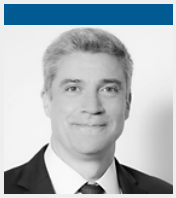
DIRETORA-PRESIDENTE

Julia Dias Leite

Diretora-Presidente do CEBRI. Atua há 20 anos na área de Relações Internacionais. Ocupou cargos de direção nas principais instituições independentes do setor no Brasil e desenvolveu relacionamento com representantes da iniciativa privada, governos e entidades oficiais nacionais e no exterior, em especial da América do Sul, Estados Unidos e Ásia. Dentre elas, foi Secretária Executiva do Conselho Empresarial Brasil-China (CEBC). Formada em Direito pela Universidade Cândido Mendes e com MBA em Gestão de Negócios pela FGV, colaborou na área de pesquisas com o Council of the Americas, em Nova York. É *Fellow* do Inter-American Dialogue e, em 2017, foi a representante brasileira no International Visitor Leadership Program, do Departamento de Estado americano. É Presidente do Conselho de Administração da Piemonte Holding.

Participantes do 1º Webinar do Grupo Cyber

25 de agosto de 2020



André Clark

Conselheiro do CEBRI e General Manager da Siemens Energy no Brasil

Daniel Sales Correa

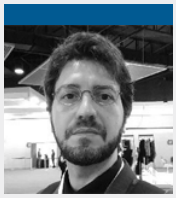
Vice-Presidente de Investimentos & Tecnologias Digitais na Braskem S/A

Arthur Pereira Sabbat

Coronel da Reserva do Exército Brasileiro, Diretor do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI-PR)

Luciana Gama Muniz

Diretora de Projetos do CEBRI



Bruno Daniel Mazeto

Especialista em Regulação da Superintendência de Regulação dos Serviços de Transmissão (SRT) da Agência Nacional de Energia Elétrica (ANEEL)

Mário Luiz Silvério

Diretor Presidente da Companhia Paulista de Desenvolvimento (CPD)

Paulo Sergio Melo de Carvalho

Senior Fellow do CEBRI e General de Divisão da Reserva do Exército Brasileiro

Sumário Executivo

Uma série de eventos ocorridos na atualidade tornaram as pessoas ainda mais dependentes do mundo digital e, consequentemente, todos os Estados-Nação devem estar especialmente atentos à **proteção dos seus ativos de informação**, sejam públicos ou privados.

No Brasil, onde a população em geral é aficionada pela internet e, principalmente, pelas redes sociais, os órgãos governamentais e as empresas públicas têm buscado soluções para facilitar a utilização das benesses do mundo digital, preocupando-se, de forma elementar, com a proteção das suas redes de dados, especialmente com o **trânsito da informação entre o mundo corporativo e as residências dos usuários**.

Com a chegada da **COVID-19** e a disseminação do trabalho remoto, o dito "***home office***", as pessoas vêm demandando mais facilidades na internet, que tornem a sua vida mais amena, minimizando os desconfortos das limitações de mobilidade impostas por esta inusitada pandemia.

Esta aproximação interpessoal no ambiente virtual tem facilitado os **ataques cibernéticos**, com destaque para as ações relacionadas com o **mundo dos negócios**, impondo que as empresas invistam em tecnologia da informação e comunicações.

No setor governamental, especial atenção deve ser dada às **infraestruturas críticas**, pois são gerenciadas – tanto na parte operacional, como no setor administrativo – por sistemas digitais, sendo assim, sujeitas às ameaças cibernéticas.

Um exemplo atual está relacionado com os Estados Unidos da América, onde qualquer **projeto do setor energético de alta criticidade**, para sua entrada naquele país, deve ser objeto de rigorosa avaliação na área de segurança cibernética.

No Brasil, diversas **empresas do setor energético têm sofrido sérios ataques cibernéticos** que dificultam a sua operação e impõem a adoção de estratégias para minimizar os riscos e danos destes ataques ao seu negócio, que se refletem diretamente no dia-a-dia da população e, consequentemente, são tema relevante de segurança nacional.

Os setores envolvidos com as infraestruturas críticas nacionais – energia, transporte, água, telecomunicações e finanças – têm procurado desenvolver programas para aperfeiçoar a segurança cibernética dos seus ativos de informação, onde merece realce aqueles voltados para a **sensibilização e conscientização de todos os seus colaboradores**, desde os executivos até os envolvidos com os setores operacionais, ou seja, aqueles que trabalham no "chão de fábrica" e são fundamentais para o êxito dos negócios.

Nesta área de atuação, ressalta-se uma grande demanda pelos especialistas de tecnologia da informação, comunicações e cibernética, num cenário em que as empresas oferecem vagas para os **talentos cibernéticos**, mas o mercado de recursos humanos em nosso país não possui profissionais com as habilitações necessárias para enfrentar as ameaças que partem da engenhosidade e da criatividade dos *hackers*.

As **ameaças cibernéticas** estão dinamizadas neste período de pandemia, com as pessoas trabalhando em casa e tendo necessidade de comunicar-se pela internet, criando um terreno fértil para a disseminação dos ataques cibernéticos e impondo a **adoção de medidas de segurança cibernética pelos órgãos governamentais e privados**.

O Gabinete de Segurança Cibernética da Presidência da República (GSI-PR), por intermédio do Departamento de Segurança da Informação, tem dinamizado as ações relacionadas com a proteção dos **ativos de informação da Administração Pública Federal (APF)** incrementando o **arcabouço normativo** para facilitar as atividades de cooperação entre os diversos entes do Estado, sejam federais, estaduais ou municipais, com especial atenção para as infraestruturas críticas nacionais.

Neste sentido, com relação ao setor energético, a Agência Nacional de Energia Elétrica (ANEEL) busca **regulamentar a segurança cibernética** entre os diversos operadores do sistema elétrico, de modo a promover as medidas preventivas e dinamizar as atividades de colaboração, principalmente para reduzir os riscos e danos causados pelos incessantes e contínuos ataques cibernéticos ao setor energético.

O Estado não realiza uma eficiente, eficaz e efetiva atividade de segurança cibernética sem contar com o apoio dos recursos de tecnologia da informação, comunicações e cibernética dos entes privados. A **atividade colaborativa** é de vital importância para a segurança cibernética, impondo a necessidade de um trabalho participativo que envolve vários atores, sejam governamentais ou privados.

Há necessidade de serem buscados mecanismos que possibilitem o trabalho colaborativo entre os órgãos governamentais e empresas na área de segurança cibernética, e de serem realizados estudos para viabilizar a **implementação de concessões** para empresas privadas atuarem com o Estado neste sensível, crítico e estratégico setor para a segurança nacional.

A Segurança Cibernética na Sociedade Brasileira

Em tempos de pandemia da COVID-19, a adesão ao trabalho de "*home office*" deixou de ser gradual para ter características de uma situação de emergência em virtude de as pessoas terem a obrigatoriedade de realizar o teletrabalho.

Criou-se uma realidade delicada para os setores empresariais, comerciais e industriais, gerando desafios e fazendo surgir vulnerabilidades nos sistemas digitais uma vez que a plataforma de ataque aumentou imensamente. Incrementou-se vertiginosamente a dependência das pessoas em relação à internet – já que muitas atividades deixaram de ser realizadas presencialmente – e elas tornaram-se vulneráveis, em diversos graus e sentidos.

É interessante ressaltar que os requisitos para o sucesso de um ataque cibernético são, a saber: ferramentas, habilidade, motivação, conhecimento e oportunidade – e, para aqueles que estão se defendendo das ameaças cibernéticas, resta trabalhar no requisito oportunidade, precavendo-se e reduzindo os riscos e vulnerabilidades por intermédio de metodologias e ferramentas que são utilizadas pelas empresas.

O Governo Federal não está alheio a estas iniciativas, e muito tem sido feito para minimizar estes danos, com ações efetivas buscando sensibilizar a sociedade brasileira, pois é impossível o governo garantir segurança cibernética sozinho, sem contar com o apoio colaborativo de órgãos públicos e privados, e, até mesmo, das pessoas individualmente.

Uma iniciativa importante do GSI-PR ocorreu antes do período da pandemia da COVID-19. Trata-se da Estratégia Nacional de Segurança Cibernética, emitida pelo Decreto número 10.220, de 5 de fevereiro do corrente ano, o qual, apesar de ter caráter mandatório de decreto, tem sido trabalhado pelo governo de forma recomendatória, estabelecendo grandes rumos para a realização de segurança cibernética a nível nacional e buscando focar nos requisitos de

resistência e resiliência das atividades de proteção dos ativos de informação estratégicos da sociedade brasileira.

O GSI-PR está empenhado na elaboração de um decreto que efetive a criação do Sistema Federal de Incidentes Cibernéticos, congregando todas as Equipes de Prevenção e Resposta de Incidentes Cibernéticos da administração pública federal. Trata-se de um modelo que se pretende implementar para facilitar a elaboração de um instrumento mais abrangente, que é a Política Nacional de Segurança Cibernética, a qual permitirá uma maior participação dos setores representativos da sociedade brasileira, tais como a Academia e as empresas, e possibilitará uma maior sinergia com os projetos governamentais de segurança cibernética.

Esta política irá direcionar os trabalhos para a criação de um grande pacto nacional – integrando uma concertação de atores diversos, para fortalecer a cultura e a maturidade da segurança cibernética brasileira, estabelecendo programas de sensibilização e conscientização a nível nacional – bem como criar um sistema que estabeleça requisitos básicos e essenciais de segurança cibernética.

O seu esforço principal será no aspecto educacional, buscando criar na sociedade brasileira a cultura de segurança cibernética, iniciando o trabalho de busca de talentos entre as crianças e aperfeiçoando os adultos na metodologia de utilização de procedimentos básicos dos sistemas e ferramentas computacionais, o que reduzirá o número de ataques cibernéticos bem-sucedidos no cenário brasileiro.

O coroamento da execução desta política dar-se-á com a criação do Sistema Nacional de Segurança Cibernética, instrumento fundamental para a efetivação de uma cultura de segurança cibernética e para a realização de ações mais efetivas entre os diversos atores da sociedade brasileira na proteção dos ativos de informação públicos e privados. Contará, ainda, com um Conselho Nacional de Segurança Cibernética para assessorar o presidente da república nesta área temática.

No âmbito internacional, o GSI-PR busca realizar acordos de cooperação com diversos países, estabelecendo memorandos de entendimento que possibilitarão o compartilhamento de informações relacionadas com as ameaças cibernéticas, as tendências de crime e ataques cibernéticos, as vulnerabilidades latentes, os novos *malwares* e o intercâmbio na metodologia da prevenção e resposta a incidentes cibernéticos.

Desse modo, todas estas iniciativas, incluindo os acordos de cooperação internacionais, buscam efetivar medidas de construção de confiança entre os diversos atores de um latente sistema nacional de segurança cibernética, o qual contribuirá para uma maior resiliência nas atividades de defesa frente aos ataques cibernéticos, envolvendo ações colaborativas entre órgãos públicos e privados, bem como aperfeiçoar a consciência brasileira de segurança cibernética.

A Intervenção Regulatória e a Segurança Cibernética no Setor Elétrico

A Agência Nacional de Energia Elétrica (ANEEL) vem trabalhando desde 2015 na sensibilização dos entes da sua área de atuação em uma tarefa complexa que é a intervenção regulatória e a segurança cibernética no setor elétrico.

A tarefa é complexa pela diversidade do setor elétrico e por ele possuir características essenciais, por exemplo, em relação aos serviços – geração, transmissão e distribuição. Tratam-se de atividades bem diferentes, as quais possuem características próprias e um modelo único com sistemas econômicos diferentes: na geração o sistema é concorrencial, enquanto na distribuição é monopolista e na transmissão pode ser qualquer um dos dois sistemas, sendo, no Brasil, adotado o monopolista.

As empresas do sistema elétrico têm modos diferentes de atuação, sendo umas privadas e outras estatais, além de poderem ser federais, estaduais ou municipais. Existem, ainda, empresas estatais de outros países que atuam no Brasil como se fossem privadas.

Outro ente importante são os sistemas isolados, os quais atendem comunidades e onde, por exemplo, a pane de um gerador pode causar sérios danos no dia-a-dia das pessoas.

O comércio de energia é realizado por comercializadoras, com características financistas e reguladas pelo Banco Central, apesar de gerenciarem comercialmente a energia de todo o país.

O setor elétrico possui três órgãos importantes para o seu funcionamento, a saber: a Câmara de Comercialização de Energia Elétrica (CCEE), responsável pela operação do mercado de energia; o Operador Nacional do Sistema Elétrico (ONS), que cuida da coordenação e controle da operação das instala-

ções de geração e transmissão; e a Empresa de Pesquisa Energética (EPE), que tem a finalidade de realizar estudos e pesquisas para o planejamento do setor energético.

Estes três órgãos lidam com informações críticas, que merecem contar com as medidas de segurança cibernética, e caracterizam também a heterogeneidade do setor elétrico, além de poderem impactá-lo de forma determinante caso sejam objeto de ataques cibernéticos.

A principal característica do setor elétrico é sua heterogeneidade e diversidade de requisitos. Por exemplo, conta com distribuidoras que atendem até mil consumidores, enquanto existem outras que possuem onze milhões de clientes; algumas têm receita de um milhão de reais e outras contam com doze bilhões de arrecadação; e algumas têm geração de um megawatt enquanto a usina hidrelétrica de Itaipu gera em torno de quatorze gigawatts.

Portanto, a realização da intervenção regulatória em segurança cibernética no setor elétrico exige que a equipe de especialistas compreenda a diversidade deste setor, trabalhando com diferentes parâmetros que vão do tipo de consumidor, passam pela receita anual e podem chegar à potência instalada.

A ANEEL tem procurado discutir esta intervenção com todos os entes do setor, inclusive, com representantes da sociedade, buscando subsídios para torná-la robusta e eficaz, realizando também conversações com a Agência Nacional de Telecomunicações (ANATEL) e o Banco Central, que já estão em estágios mais avançados nas suas regulamentações.

Estas iniciativas buscam identificar os desafios, as dificuldades e as boas práticas para executar essa complexa tarefa de intervenção regulatória, pois a Tecnologia Operacional (TO) do setor energético não caminhou junto com os avanços da segurança cibernética, diferentemente da Tecnologia da Informação (TI), que foi incrementada para atender às necessidades prementes da segurança cibernética.

Estão sendo buscados contatos com os Estados Unidos da América e com a União Europeia para analisar os modelos por eles adotados e trazer ensinamentos para facilitar a elaboração dos documentos que balizam a regulamentação em questão.

Enfim, os desafios para esta intervenção regulatória de segurança cibernética no setor elétrico passam pelo(a):

- necessidade de definição concreta das infraestruturas críticas do setor elétrico com requisitos práticos e mensuráveis;
- estabelecimento de confiança entre os entes do setor para que as vulnerabilidades existentes não sejam usadas para aplicação de multas;
- intercâmbio de informações para melhorar o seu sistema de proteção contra ataques cibernéticos;
- implementação de um eficiente sistema de certificação para aperfeiçoar a qualificação profissional; e
- execução de um contínuo e constante programa de sensibilização de segurança cibernética.

A Segurança Cibernética no ambiente dos Acordos de Cooperação

Os acordos de cooperação na área da segurança cibernética são fortemente dependentes da relação entre o setor público e a iniciativa privada, como pode ser depreendido do que ocorre no mundo agora, com a pandemia da COVID-19, quando a produtividade das empresas – sejam públicas ou privadas – foi altamente afetada pela sua dependência da internet, principalmente no que se refere aos seus processos.

O GSI-PR tem buscado regular o setor cibernético com a emissão de documentos normativos, o que vem influenciando os demais setores governamentais que dependem decisivamente dos meios computacionais na realização de ações similares.

Isto permitirá ao Brasil um maior conforto nas relações internacionais, ficando em igualdade com os demais países, além de facilitar as diversas atividades no âmbito nacional, incluindo a segurança nacional.

Um caso de sucesso no setor público, de parceria público-privada, encontra-se em Brasília, envolvendo o compartilhamento do datacenter de dois grandes bancos: o Banco do Brasil e a Caixa Econômica Federal, onde foram utilizados recursos privados para a aquisição dos equipamentos e execução do suporte operacional, e os dois bancos trabalharam intensamente na área de inteligência cibernética.

A competência do setor público para os acordos de cooperação na área de segurança de cibernética deve caminhar para estabelecer mecanismos de regulação e acompanhamento dos processos e metodologias, enquanto o setor privado deve contribuir com o capital intelectual, as ferramentas e o investimento.

O governo deve estabelecer um sistema de certificação com regras próprias para facilitar o trabalho diversificado de empresas privadas, evitando a ocor-

rência de monopólios. O setor privado deve buscar conciliar os interesses públicos, trazendo os investimentos para desenvolver tecnologia e compartilhar conhecimentos.

O segredo do sucesso nos acordos de cooperação no setor cibernético é incentivar que os diversos atores interajam em um ambiente colaborativo, com o governo executando a certificação sem limitar a criatividade dos especialistas, o que é fundamental para realizar a proteção dos ativos de informação frente aos constantes e contínuos ataques, onde a operação dos diversos sistemas computacionais sempre será o elo mais fraco na cadeia da segurança cibernética.

Assim, o modelo de acordos de cooperação no setor cibernético conduz para um sistema híbrido, onde o setor privado deve desenvolver as ferramentas, realizando o investimento e a operação, enquanto o governo deve ser o ente regulador e coordenador.

Os desafios da Segurança Cibernética no meio empresarial energético

Os crimes cibernéticos são os maiores riscos aos negócios das empresas em todo o mundo, apenas ficam atrás das ações decorrentes de desastres naturais, relacionados com a escassez de água e com as grandes questões ocasionadas pelas condições climáticas.

As questões de segurança cibernética são facilitadas nas empresas quando a Tecnologia das Operações (TO) e a Tecnologia da Automação (TA) acompanham os avanços da Tecnologia da Informação (TI), com processos bem definidos e uma grande integração entre estas tecnologias, minimizando os riscos decorrentes do relacionamento com o mundo digital.

Os ataques cibernéticos podem causar sérios danos nas empresas energéticas, tais como a desativação total dos seus meios operacionais, inutilização de equipamentos e interrupção de serviços, principalmente pela existência, na atualidade, de sistemas digitais com controles distribuídos, o que obriga o acompanhamento destas ameaças em tempo real.

Esta grande digitalização das plantas energéticas impõe a necessidade de um controle avançado nas pontas e nas diversas camadas dos seus sistemas, o que implica a realização de políticas bem definidas e uma gestão rígida da governança dos seus ativos de informação, facilitando a operação dos diversos sistemas da empresa.

Isto demanda um monitoramento constante destes ativos com processos muito bem definidos, com respostas preparadas para os diversos ataques cibernéticos, buscando parcerias, inclusive no exterior, para implementá-las.

Como uma referência do avanço dos ataques cibernéticos na atualidade, podemos citar a seguinte pesquisa: dos dez bilhões e setecentos mil eventos de natureza cibernética ocorridos, no mês de julho do corrente ano em uma

empresa energética, setecentos e cinquenta geraram alertas nos sistemas de controle; quatrocentos e quarenta tinham criticidade; e, finalmente, trinta e cinco configuraram incidentes de segurança.

Constata-se a importância da gestão e do tratamento dos incidentes cibernéticos, principalmente pelo fato de que as empresas, além de gerirem suas próprias informações, lidam também com os dados de fornecedores e clientes, e sua utilização indevida pode causar danos imensuráveis a todos os entes envolvidos no negócio.

A ação devastadora dos ataques cibernéticos implica que nenhuma empresa está totalmente segura nesta área, o que impõe um trabalho contínuo nas diversas tecnologias – TO, TA e TI – que resulte em processos bem definidos e com colaboradores conscientes e sensibilizados para a importância de seguir procedimentos que permitam uma proteção eficiente, eficaz e efetiva dos seus ativos de informação.

Comentários finais

Na atualidade, os executivos de empresas devem se preocupar com o cenário cibernético, onde prosperam ataques que colocam em risco os seus negócios, podendo levar as suas organizações à falência, além de os colocar em situação crítica em termos de responsabilidade fiduciária.

A gestão dos incidentes cibernéticos, para os executivos das empresas, está no mesmo patamar do gerenciamento de crise decorrente de acidente ambiental. Não pode ser descuidada, e os Estados-Nação estão buscando mecanismos para regulamentá-la, criando leis que convirjam para a integração dos entes públicos e privados para a proteção dos ativos de informação, e impondo responsabilidades para os seus executivos.

O Brasil vive este cenário, onde o GSI-PR esforça-se para estabelecer normas que minimizem os danos causados pelos ataques cibernéticos pela falta de alinhamento das ações estratégicas executadas pelos órgãos da administração pública federal na segurança cibernética com as ações táticas realizadas pelos seus centros de tratamentos e resposta a incidentes.

A internet não se autorregula e o incremento das fraudes em tempos de pandemia da COVID-19 reforça a necessidade de o governo brasileiro aperfeiçoar seus mecanismos de gestão da segurança cibernética, criando com brevidade o Sistema Federal de Incidentes Cibernéticos. Esse sistema deverá ser um órgão regulador, mas contará também com ações executivas, coordenadas e colaborativas, entre os diversos entes envolvidos, sejam públicos ou privados.

No cenário mundial, os empresários desejam fazer negócios em locais seguros, onde o privado coopera com o público, minimizando os riscos e danos causados pelos ataques cibernéticos, e exista uma convergência e, até mesmo, uma integração das atividades de segurança cibernética, o que demanda um maior investimento de recursos financeiros.

O setor energético não é diferente dos outros setores e, sendo assim, a ANEEL deve atuar como agente regulador junto às diversas empresas de energia - geração, distribuição e transmissão - sem se olvidar do papel fundamental de possuir, inclusive, um centro de tratamento e resposta de incidentes, que centralizará as ações de proteção das diversas empresas em um ambiente de cooperação, contribuindo para tornar o seu sistema resiliente às ameaças cibernéticas e criar a mentalidade de local seguro para os empresários investirem.

O Brasil caminha para a tecnologia 5G, e o governo já emitiu normas estabelecendo requisitos mínimos para sua implantação e operação, atendendo às demandas geopolíticas, mercadológicas, comerciais, de segurança e de relações exteriores. Entretanto, a sociedade brasileira precisa ter uma participação maior para trabalhar junto com os seus servidores do Estado, estabelecendo um modelo que transcenda as nossas fronteiras e possua atratividade para os negócios.

Há necessidade de o país melhorar a sua consciência situacional em relação aos incidentes cibernéticos. Essa atividade não deve ser apenas uma obrigação do governo, mas envolve todos os setores da sociedade, desde as empresas que trabalham com as infraestruturas críticas nacionais, até aquelas que são ilhas de excelência na gestão da segurança cibernética, impondo o estabelecimento de acordos de cooperação, nos quais o privado ajude o público a cumprir com suas obrigações governamentais, em um ambiente de colaboração e confiança.

CEBRI
CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

Associados

Instituições

Abiquim
Aegea
Aeróleo Táxi Aéreo
BAMIN
Banco Bocom BBM
BASF
BMA Advogados
BDMG
BNDES
BRF
Brookfield Brasil
Bunker One
Captalys Investimentos
CCCC/Concremat
Comerc Energia
Consulado Geral dos Países Baixos no Rio de Janeiro
Consulado Geral da Irlanda em São Paulo
Consulado Geral do México no Rio de Janeiro
Consulado Geral da Noruega no Rio de Janeiro
CTG Brasil
Dannemann, Siemsen, Bigler & Ipanema Moreira
Dynamo
EDP
Eletrobras
Embaixada da China no Brasil
ENEVA
ENGIE Brasil
Equinor
ExxonMobil
FCC S.A.
Grupo Lorentzen
Grupo Ultra
Huawei
IBÁ
IBRAM
Icatu Seguros
InvestHK
Ipanema Investimentos
Itaú Unibanco
JETRO
Klabin
Lazard
Light
Mattos Filho Advogados
Museu do Amanhã
Michelin
Neoenergia
Oktri Empreendimentos
Paper Excellence
Petrobras
Pinheiro Neto Advogados
Prumo Logística
Repsol Sinopec
Sanofi
Santander
Shell
Siemens Energy
Souza Cruz
SPIC Brasil
State Grid
Tecnoil
Total E&P do Brasil
Vale
Veirano Advogados
Vinci Partners

Senior Fellows

Adriano Proença
Ana Célia Castro
Ana Paula Tostes
André Soares
Benoni Belli
Carlos Milani
Clarissa Lins
Daniela Lerda
Denise Nogueira Gregory
Diego Bonomo
Evangelina Seiler
Fabrizio Sardelli Panzini
Fernanda Guardado
Fernanda Magnotta
Hussein Kalout
Izabella Teixeira
Larissa Wachholz
Leandro Rothmuller
Lia Valls Pereira
Mário Ripper
Matias Spektor
Miguel Correa do Lago
Monica Herz
Patrícia Campos Mello
Paulo Sergio Melo de Carvalho
Pedro da Motta Veiga
Philip Yang
Ricardo Sennes
Rogerio Studart
Sandra Rios
Tatiana Rosito
Vera Thorstensen
Victor do Prado

Equipe CEBRI

Diretora-Presidente
Julia Dias Leite

Diretora Relações Institucionais e Comunicação
Carla Duarte

Diretora de Projetos
Luciana Gama Muniz

Projetos

Gerente de Projetos
Lara Azevedo

Consultoras
Cintia Hoskinson
Marianna Albuquerque

Estagiários
Gustavo Berlie
Larissa Vejarano

Relacionamento Institucional e Eventos

Gerente de Relações Institucionais e Eventos
Barbara Brant

Consultores
Caio Vidal
Nana Villa Verde

Estagiário
Lucas Bilheiro

Comunicação

Consultora
Gabriella Cavalcanti

Estagiário
Henrique Kress

Administrativo e Financeiro

Coordenadora Adminstrativa-Financeira
Fernanda Sancier

Assistente
Kelly C. Lima

CEBRI
CENTRO BRASILEIRO DE
RELAÇÕES INTERNACIONAIS

ONDE ESTAMOS:

Rua Marquês de São Vicente, 336
Gávea, Rio de Janeiro – RJ - Brazil
22451-044

Tel: +55 (21) 2206-4400

cebri@cebri.org.br

www.cebri.org