Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal

2015 - 2018

Versão 1.0

Presidenta da República
Dilma Rousseff

Vice-Presidente da República
Michel Temer

Ministro de Estado Chefe do Gabinete de Segurança Institucional
José Elito Carvalho Siqueira

Secretário Executivo do Conselho de Defesa Nacional
José Elito Carvalho Siqueira

Secretário Executivo do Gabinete de Segurança Institucional
Geraldo Antonio Miotto

Diretor do Departamento de Segurança da Informação e Comunicações
Marconi dos Reis Bezerra

Presidência da República
Gabinete de Segurança Institucional
Secretaria-Executiva
Departamento de Segurança da Informação e Comunicações

ESTRATÉGIA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES E DE SEGURANÇA CIBERNÉTICA DA ADMINISTRAÇÃO PÚBLICA FEDERAL

2015-2018

Versão 1.0

Brasília – DF
2015

Grupo Técnico de Elaboração da Estratégia
(Boletim Interno GSI/PR nº 52, de 26/12/2014. SE/GSI/PR Gen. Edson Leal Pujol)
Departamento de Segurança da Informação e Comunicações
Marconi dos Reis Bezerra (Coordenador)
Alcimar Sanches Rangel
Alexandre José Ribeiro
Antônio Magno Figueiredo de Oliveira
Claudia Canongia
Gustavo Andrade Bruzzeguez
Josita Arcanjo Ramos Ferreira
Lucas de Oliveira Souto
Marcelo de Almeida Maymone
Marlene Isidro da Silva
Wagner Barp Meyer

Capa: Alcimar Sanches Rangel
Normalização bibliográfica: Biblioteca da Presidência da República

Colaboração: Membros do Comitê Gestor de Segurança da Informação – CGSI/CDN
Portaria SE/CDN nº 07, de 17 de março de 2015
(DOU nº 52; 18/03/2015)

Ficha Catalográfica
Dados Internacionais de Catalogação na Publicação (CIP)

B823e Brasil. Presidência da República. Gabinete de Segurança Institucional.
Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018 : versão 1.0 / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília : Presidência da República, 2015.
82 p. : il.

ISBN

1. Segurança da informação. 2. Segurança Cibernética. 3. Administração Pública Federal. I. Título.

CDD 005.8

Ficha Catalográfica produzida pela Biblioteca da Presidência da República

[A Portaria SE/CDN No. 14, de 11 de maio de 2015, publicada no DOU No. 88 de 12/05/2015, homologa esta Estratégia]

“O planejamento é uma das maiores conquistas libertárias que o homem pode almejar. Porque o plano é a tentativa do homem para criar seu futuro; é lutar contra as tendências e correntes que nos arrastam; é ganhar espaço para escolher; é mandar sobre os fatos e as coisas para impor a vontade humana; é recusar-se a aceitar o resultado social que a realidade atomizada de infinitas ações contrapostas oferece-nos anarquicamente; é rejeitar o imediatismo; é somar a inteligência individual para multiplicá-la como inteligência coletiva e criadora.”

Carlos Matus

"Gestão Pública é um campo de conhecimento peculiar. Trata-se de uma área por definição interdisciplinar e que depende de conhecimento advindo da ciência política, da economia, da administração, da sociologia, do direito, da história e da cibernética. Acrescente-se aí o forte componente aplicado do aprendizado."

Fernando Abrúcio & Francisco Gaetani

"Uma agenda de longo prazo para reformar a gestão pública brasileira depende, como em qualquer outro campo de políticas públicas, não só de ideias e análises. Acima de tudo, é preciso constituir coalizões. Atores estratégicos precisam ser convencidos da centralidade dessa questão, como já o foram em outros tópicos."

Fernando Abrúcio

SUMÁRIO

LISTA DE SIGLAS

ABIN: Agência Brasileira de Inteligência

ABNT: Associação Brasileira de Normas Técnicas

AGU: Advocacia-Geral da União

ANATEL: Agência Nacional de Telecomunicações

APF: Administração Pública Federal

BB: Banco do Brasil

BCB: Banco Central do Brasil

BSC: *Balanced Scorecard*

CEPESC: Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações

CC/PR: Casa Civil da Presidência da República

CDCiber/MD: Centro de Defesa Cibernética / Ministério da Defesa

CDN: Conselho de Defesa Nacional

CEF: Caixa Econômica Federal

CEGSIC: Curso de Especialização em Gestão de SIC

CGI.br: Comitê Gestor da Internet no Brasil

CGSI: Comitê Gestor da Segurança da Informação

CGU: Controladoria-Geral da União

COMAER/MD: Comando da Aeronáutica / Ministério da Defesa

ComDCiber: Comando de Defesa Cibernética

CPI: Comissão Parlamentar de Inquérito

CREDEN: Câmara de Relações Exteriores e Defesa Nacional

CTIR Gov: Centro de Tratamento de Incidentes de Redes da Administração Pública Federal

DAS: Cargo do Grupo-Direção e Assessoramento Superiores

DATAPREV: Empresa de Tecnologia e Informações da Previdência Social

DSIC: Departamento de Segurança da Informação e Comunicações

DPDT: Departamento de Pesquisa e Desenvolvimento Tecnológico

EAD: Ensino à distância

EB/MD: Exército Brasileiro / Ministério da Defesa

EED: Empresa Estratégica de Defesa

EGTI: Estratégia Geral de Tecnologia da Informação

EGTIC: Estratégia Geral de Tecnologia da Informação e Comunicações

Embrapa: Empresa Brasileira de Pesquisa Agropecuária

EnaDCiber: Escola Nacional de Defesa Cibernética

ENAP: Escola Nacional de Administração Pública

END: Estratégia Nacional de Defesa

ETIR: Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais

GSI/PR: Gabinete de Segurança Institucional da Presidência da República

GTI: Grupo de Trabalho Interministerial

ICP-Brasil: Infraestrutura de Chaves Públicas Brasileira

ICT: Instituição de Ciência e Tecnologia

IEC*: International Electrotechnical Commission*, Comissão Eletrotécnica Internacional

IN: Instrução Normativa

INSS: Instituto Nacional do Seguro Social

ISO: *International Organization for Standardization*, Organização Internacional de Normalização

LAI: Lei de Acesso à Informação

MB/MD: Marinha do Brasil / Ministério da Defesa

MC: Ministério das Comunicações

MCTI: Ministério da Ciência, Tecnologia e Inovação

MD: Ministério da Defesa

MDIC: Ministério do Desenvolvimento Indústria e Comércio Exterior

MEC: Ministério da Educação e Cultura

MJ: Ministério da Justiça

MP: Ministério do Planejamento, Orçamento e Gestão

MPS: Ministério da Previdência Social

MRE: Ministério das Relações Exteriores

MS: Ministério da Saúde

MTur: Ministério do Turismo

NBR: Normas Brasileiras de Referência

NC: Norma Complementar

NSC: Núcleo de Segurança e Credenciamento

OE: Objetivos Estratégicos

OEA: Organização dos Estados Americanos

OGS: Órgão Governante Superior

PDCA: *Plan, Do, Check & Act*.

PDTI: Plano Diretor de Tecnologia da Informação

Petrobrás: Petróleo Brasileiro S.A.

PNAD: Pesquisa Nacional por Amostra de Domicílios

POSIC: Política de Segurança da Informação e Comunicações

PR: Presidência da República

Radiobrás: Empresa Brasileira de Radiodifusão

RENASIC: Rede Nacional de Excelência em Segurança da Informação e Criptografia

RNP: Rede Nacional de Ensino e Pesquisa

SAE/PR: Secretaria de Assuntos Estratégicos da Presidência da República

SECOM/PR: Secretaria de Comunicações da Presidência da República

SegCiber: Segurança Cibernética

SERPRO: Serviço Federal de Processamento de Dados

SG/PR: Secretaria-Geral da Presidência da República

SIC: Segurança da Informação e Comunicações

SICGov: Congresso de Segurança da Informação e Comunicações

SISP: Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo federal

SPOA: Subsecretaria de Planejamento, Orçamento e Administração

SRF: Secretaria da Receita Federal

SRP: Secretaria da Receita Previdenciária

TCU: Tribunal de Contas da União

TELEBRÁS: Telecomunicações Brasileiras S.A.

TIC: Tecnologias de Informação e Comunicação

UIT: União Internacional de Telecomunicações

UnB: Universidade de Brasília

WCIT: *World Conference on International Telecommunications,* Conferência Mundial em Telecomunicaçoes Internacionais

APRESENTAÇÃO

É com grande satisfação que apresento a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0", dado que tais áreas são consideradas como questões nacionais, horizontais e estratégicas, que afetam todos os níveis da sociedade, e representa importante instrumento de apoio ao planejamento dos órgãos e entidades do Governo, objetivando melhorar sobremaneira a segurança e a resiliência das infraestruturas críticas e dos serviços públicos nacionais.

Este instrumento de apoio ao planejamento estratégico governamental complementa a Instrução Normativa GSI/PR 01/2008, reúne um conjunto de objetivos estratégicos e metas para os próximos quatro anos, e visa a busca da excelência da Segurança da Informação e Comunicações (SIC) e da Segurança Cibernética (SegCiber) no âmbito da Administração Pública Federal (APF) do País, contemplando relevantes aspectos, dada a complexidade e a dinâmica de tais temas no cenário atual, nacional e mundial.

Assim, a elaboração desta Estratégia é motivada pela missão do GSI/PR de coordenar as atividades de segurança da informação do governo e considera tanto a necessidade ímpar de assegurar ações efetivas nestas áreas, quanto a possibilidade real e crescente de uso das Tecnologias de Informação e Comunicação (TIC) para ações ofensivas e exploratórias, entre outras, acesso indevido às redes de computadores de setores e de infraestruturas críticas.

Destaco ainda a ameaça relativa à elevada interconectividade mundial entre os maiores desafios da atualidade, confirmadas pelo *World Economic Forum* em suas análises sobre os riscos globais, tanto em 2014 quanto em 2015, em que são evidenciados, entre os grandes riscos tecnológicos, os ataques a redes e infraestruturas críticas da informação; o aumento dos ataques cibernéticos; e os incidentes de fraudes e roubos de dados.

Diante da criticidade desse cenário e da recomendação do Tribunal de Contas da União (TCU), no Acórdão 3.051/2014-TCU-Plenário, de que este GSI/PR lançasse Estratégia no âmbito da sua jurisdição, pautada nos pilares consagrados da segurança da informação – disponibilidade, integridade, confidencialidade e autenticidade -, com o objetivo de fortalecer as ações de SIC e de SegCiber na APF, foi instituído Grupo de Trabalho interno, no final do ano de 2014, no âmbito do Departamento de Segurança da Informação e Comunicações (SIC) deste GSI/PR para elaborar esta Estratégia.

Cabe ressaltar que o Comitê Gestor de Segurança da Informação (CGSI), órgão de assessoramento da Secretaria Executiva do Conselho de Defesa Nacional, a qual é exercida por este GSI/PR, em temas relativos à segurança da informação e correlatos, conforme disposto no Decreto nº 3.505/2000, vem colaborando efetivamente nos últimos anos com o arcabouço normativo das áreas de SIC e de SegCiber, e foi

consultado, contribuindo substantiva e efetivamente com esta publicação, ao que desde já agradeço a colaboração.

Sabemos que ainda há muito a ser alcançado e que estamos passo a passo criando as condições necessárias para maior efetividade, eficácia e eficiência das ações de SIC e de SegCiber, principalmente no que diz respeito ao entendimento das novas exigências para a manutenção e preservação tanto das infraestruturas críticas do País, quanto dos direitos individuais, em especial da privacidade, protegendo e assegurando os interesses da sociedade e do Estado.

Recomendo, portanto, a leitura e a aderência aos objetivos estratégicos e metas desta "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015 – 2018, versão 1.0" na direção do fortalecimento e da excelência da segurança da informação e comunicações e da segurança cibernética no Governo.

Considero esta publicação um importante incremento ao arcabouço de documentos que objetivam contribuir com a segurança institucional e a soberania nacional, e convido-os a contribuir com propostas e sugestões para a evolução contínua da mesma, visando construir, em futuro próximo, de forma colaborativa, a "Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética".

Por fim, cito o livro "Sonho Grande" o qual apresenta o relato da jornalista Cristiane Correa sobre a trajetória exitosa de três sócios, Jorge Paulo Lemann, Marcel Herrmann Telles e Carlos Alberto Sicupira, para o sucesso alcançado em seus empreendimentos, e aproveito para finalizar ressaltando a segunda lição do decálogo das principais lições aprendidas:

> "SUSTENTE O IMPULSO COM UM GRANDE SONHO: Gente boa precisa ter coisas grandes para fazer, senão leva sua energia criativa para outro lugar. Assim, os três construíram um mecanismo que tem duas premissas básicas: primeiro, recrute as melhores pessoas e depois dê a elas coisas grandes para fazer. Em seguida, atraia mais gente boa e proponha a próxima coisa importante a fazer. Repita o processo indefinidamente. Foi assim que eles mantiveram o ímpeto ao longo do tempo. Eles sempre vibraram com a ideia de metas grandes, arriscadas e audaciosas, e desenvolveram uma cultura para alcançá-las. Ao observá-los, aprendi que, para conservar o ímpeto e, portanto, preservar gente boa, vale a pena correr os riscos inerentes à busca pelas grandes metas. É como uma ótima equipe de alpinismo. Por um lado, existe o risco de subir uma montanha alta, depois uma montanha ainda mais alta, e depois a seguinte. Por outro lado, se você não tiver novas montanhas altas para escalar, deixará de se desenvolver e crescer, e perderá seus melhores alpinistas. Grandes alpinistas necessitam de grandes montanhas para escalar, sempre e indefinidamente".

Boa leitura! Boas práticas! "Escale"!

JOSÉ ELITO CARVALHO SIQUEIRA

Ministro de Estado Chefe do Gabinete de Segurança Institucional da

Presidência da República

CONTEXTUALIZAÇÃO

Este item apresenta, de forma geral e sem a pretensão de ser exaustivo, visão sobre avanços, mudanças, tendências e desafios da Segurança da Informação e Comunicações e da Segurança Cibernética, de 2000 até os dias de hoje, principalmente na trilha que vem sendo desenvolvida no país.

No Brasil, em 2000, o número de usuários da Internet girava em torno de 8,6 milhões e o governo brasileiro alertava que tal número era bastante limitado e precisaria crescer significativamente. Naquele ano, estimava-se que apenas 1% dos usuários da Internet no Brasil compraria em lojas virtuais, com média de gasto de apenas 18 dólares mensais (MCT, 2000).

No final de 2008, passou-se a contar com cerca de 55,9 milhões de usuários no Brasil segundo a Pesquisa Nacional por Amostra de Domicílios (PNAD) e, aproximadamente, 83 milhões de pessoas de 10 anos ou mais acessaram a Internet nos três meses anteriores à realização da PNAD em 2012, apontando para um crescimento rápido de uso da Internet no país[1]. Com relação à evolução da economia digital no país, os usuários brasileiros da Internet contribuíram com o comércio eletrônico, com faturamento da ordem de 8,2 bilhões de reais em 2008 com crescimento para cerca de 22,5 bilhões de reais em 2012, confirmando as prospecções de avanços preponderantes desta economia[2].

Em 2014, o cenário de uso da Internet e, consequentemente, de uso das Tecnologias de Informação e Comunicação (TIC) permanece crescente e sem dúvida além de qualquer expectativa e prospecção, operando-se em cifras bastante expressivas no mundo e no País, especialmente frente aos avanços do uso de dispositivos móveis, da computação em nuvem e da evolução da chamada "internet das coisas". O Brasil é considerado o quarto maior mercado mundial no setor de TIC, movimentando cerca de US$ 170 bilhões, e somente o comércio eletrônico faturou cerca de 35,8 bilhões de reais, e no mundo o movimento foi de cerca de 1,5 trilhões de dólares, demonstrando quão aquecida e intensiva vem sendo a economia digital e com tendência ascendente forte.[3] Para 2020, estima-se um mercado global de TI na ordem de US$ 3 trilhões, e um mercado nacional da ordem de US$ 200 bilhões.

Destaca-se que já foi abordado no "Livro Verde Segurança Cibernética no Brasil" (GSI/PR, 2010, p.14) os seguintes fenômenos da Sociedade da Informação: "*a) Elevada convergência tecnológica; b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos; c) Aumento*

[1] http://www.brasil.gov.br/infraestrutura/2013/09/percentual-de-internautas-cresce-nas-regioes-norte-e-nordeste-em-2012/
[2] http://www.e-commerce.org.br/stats.php
[3] Idem.

crescente e bastante substantivo de acesso à Internet e das redes sociais; d) Avanços das tecnologias de informação e comunicação (TIC); e) Aumento das ameaças e das vulnerabilidades de segurança cibernética; e, f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças"

Toda e qualquer reflexão sobre a evolução da Sociedade da Informação deve apoiar-se numa análise da mudança contemporânea da relação com o saber. A velocidade do surgimento e da renovação do conhecimento, *know-how* e tecnologias, vem sendo cada vez mais avassaladora, o que contribui para um ambiente de incertezas, volatilidade, novas e crescentes ameaças.

As ameaças relativas à elevada interconectividade mundial estão entre os maiores desafios da atualidade, confirmadas pelo *World Economic Forum* em suas análises sobre os riscos globais, tanto em 2014 quanto em 2015, em que são evidenciados, entre os grandes riscos tecnológicos, os ataques a redes e infraestruturas críticas da informação; o aumento dos ataques cibernéticos; e os incidentes de fraudes e roubos de dados.

Assim sendo, para fins desta "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética na Administração Pública Federal", são adotados os seguintes conceitos:

a) Segurança da Informação e Comunicações (SIC): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

b) Segurança Cibernética (SegCiber): a arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas;

c) Ativos de Informação: são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso; e

d) Infraestruturas Críticas: são as instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade.

A SIC e a SegCiber, portanto, vêm se caracterizando cada vez mais como função estratégica de Estado, sendo essenciais à manutenção e preservação tanto das infraestruturas críticas de um país, tais como Energia, Transporte, Telecomunicações, Águas, Finanças, a própria Informação, entre outras, quanto dos direitos individuais, em especial da privacidade, e da soberania.

Os pilares consagrados da SIC – disponibilidade, integridade, confidencialidade e autenticidade – estão sujeitos a novas e crescentes vulnerabilidades e ameaças.

São crescentes e contínuas as polêmicas nos temas regulação e controle da Internet em nível nacional e internacional. A reunião plenária "*World Conference on International Telecommunications - WCIT-12*", em Dubai, em dezembro de 2012, liderada pela União Internacional de Telecomunicações (UIT), foi marcada por divergências entre os seus Estados Membros, sendo reforçada a experiência brasileira de governança multissetorial realizada por meio de seu Comitê Gestor da Internet (CGI.br).

As questões de privacidade *versus* segurança permanecem como pontos controversos e atualmente em forte articulação, em nível nacional e internacional, em especial após o advento do "caso Snowden", que expôs possíveis ações de espionagem do governo americano em relação a outros países, Brasil inclusive, por meio da captura e tratamento de metadados na Internet. Tais questões permanecem nos debates de uso e governança da Internet, de forma preponderante, tratadas nas agendas dos governos e em fóruns bi e multilaterais.

O Governo brasileiro registrou, com satisfação, que a III Comissão da 68ª Assembleia Geral das Nações Unidas aprovou em 2013, por consenso dos 193 Estados membros, a Resolução A/RES/68/167 "O direito à privacidade na era digital"[4], a qual foi apresentada em conjunto pelo Brasil e Alemanha, em resposta às supostas denúncias de Snowden contra os EUA. "Nenhuma preocupação relacionada à segurança pública pode justificar a coleta de informações sensíveis. Estados devem garantir a observação irrestrita das suas obrigações sobre as leis internacionais de direitos humanos", diz a Resolução.

O Relatório final da Comissão Parlamentar de Inquérito, denominada CPI da Espionagem, aponta fragilidades do Brasil frente à espionagem eletrônica internacional e sugere medidas e propostas para a melhoria da segurança cibernética nacional, evidenciando a fragilidade do sistema de telecomunicações brasileiro e de nosso sistema de inteligência e defesa cibernética (Brasil. Congresso. Senado Federal, 2014).

Segundo o estudo "Mapeamento de Fornecedores Nacionais de Tecnologia da Informação e Comunicação (TIC) para Redes Elétricas Inteligentes (REI)", realizado pela Agência Brasileira de Desenvolvimento Industrial (ABDI) em 2014, a segurança cibernética foi identificada como uma das principais preocupações das concessionárias, empresas fornecedoras de TIC e centros de pesquisa voltados para o setor.

[4] http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

O cenário de realização de grandes eventos no Brasil (2013 a 2016) ressalta tais preocupações e serve de oportunidade para a conformação de uma situação benéfica, alavancando os compromissos com a SIC e com a SegCiber pactuados e reforçados na direção de que haja capacidade efetiva do governo de catalisar e estimular ações em prol dos diferentes tópicos que perpassam e sustentam tais áreas de atuação.

Cabe realçar os tópicos relativos à formação continuada de recursos humanos especializados e à capacidade de coordenação executiva no âmbito do governo, bem como àqueles que se referem ao desenvolvimento de tecnologias e à inovação, à promoção dos setores e do mercado de segurança da informação e de segurança cibernética, à construção de arcabouço legal e normativo, e à cooperação internacional.

No cenário atual, as ameaças cibernéticas são crescentes, diferenciadas e apresentam elevado grau de sofisticação, exigindo dos governos ações efetivas de prevenção e combate às práticas maliciosas no uso das TIC, por meio de ações transversais, integradoras, interdisciplinares e multissetoriais.

Nesta direção, a proteção dos ativos de informação implica na definição de investimentos para um melhor posicionamento das instituições governamentais em relação à produção e custódia, principalmente, às informações dos cidadãos brasileiros e do Estado. Assim posto, os ativos de informação guardam relação direta com riscos de SIC e de SegCiber, uma vez que a dependência tecnológica das instituições governamentais é cada vez maior.

No tocante à SIC e à SegCiber, independente das responsabilidades do Estado brasileiro, o setor privado tem importância fundamental pois detém a maior parte das infraestruturas de telecomunicações e redes de comunicação digital, provendo serviços para o Governo e para a sociedade.

Soma-se a esse cenário os desafios impostos pela forte dependência externa e pela ausência de domínio em tecnologias sensíveis de SIC e de SegCiber. Salienta-se ainda, entre os desafios, o Decreto nº 8.135/2013, que dispõe em seu art. 1º que "*as comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias*".

Observa-se também que em período recente, diversos órgãos e entidades, conforme amplamente divulgado na mídia, foram alvos de ações maliciosas, com destaque para ações de engenharia social, desfigurações de sítios, degradação dos serviços e acessos indevidos a sistemas computacionais, com exposição de

vulnerabilidades e consequente vazamento de informações, causando prejuízos ao Estado, com reflexos negativos para a sociedade.

Neste contexto, ressalta-se que não obstante os esforços do governo em fortalecer as ações de SIC e de SegCiber, o que inclui arcabouço normativo publicado pelo GSI/PR nos últimos oito anos, o respectivo nível de maturidade ainda encontra-se em patamar aquém do desejado nos órgãos e entidades da APF, segundo o Acórdão 3.051/2014-TCU-Plenário.

A Constituição Federal de 1988 estabelece amplo acesso à informação, impactando diretamente nas estratégias, políticas e atuação de todos os órgãos públicos. A publicação da Lei de Acesso à Informação (LAI) marcou uma mudança no paradigma de publicidade dos ativos de informação criados e geridos pelo Estado, em todos os níveis e esferas, em prol da transparência. Esse novo mote trouxe atenção sobre os ativos de informação sigilosos cuja publicidade seja sensível para o país. Nesse aspecto, a LAI garante tratamento diferenciado para informações cuja a exposição comprometa a segurança do Estado e da sociedade. Tal dinâmica impacta diretamente na estratégia adotada pelo governo para a SIC e a SegCiber.

Ficam, assim, evidenciados os vários desafios enfrentados pelo Governo Federal, em especial a carência do estabelecimento de governança efetiva da SIC e da SegCiber, e da segurança dos ativos de informação críticos, e a ausência de um órgão central que exerça coordenação executiva de tais temas, de forma sistêmica e participativa – "multistakeholders" e multissetores, somada a ausência de destaque orçamentário específico e adequado ao tamanho do problema.

Uma vez que SIC e SegCiber são consideradas como questões nacionais, horizontais e estratégicas, que afetam todos os níveis da sociedade, uma estratégia de SIC e de SegCiber nacional representa importante ferramenta para melhorar sobremaneira a segurança e a resiliência das infraestruturas críticas e dos serviços nacionais.

A SIC e a SegCiber têm, portanto, impactos amplos na soberania nacional, na construção da cidadania e no desenvolvimento econômico, devendo o país ser reconhecido como protagonista em nível internacional, bem como em fóruns bi e multilaterais. E, em decorrência, esforços em prol da SIC e da SegCiber podem representar um salto qualitativo e quantitativo da inserção da indústria nacional de tecnologia da informação e comunicação (TIC) nos mercados interno e global, bem como, de evolução e excelência da pesquisa, desenvolvimento e inovação dessas áreas em nível nacional e internacional.

No Brasil, os assuntos relacionados à Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de

Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, por intermédio do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que exerce as funções de Secretaria Executiva do citado Conselho e de Presidência daquela Câmara.

As competências do CDN estão previstas no art. 91 da Constituição Federal de 1988 e a regulamentação de sua organização e de seu funcionamento está contida na Lei nº 8.183/1991. As competências, organização e normas de funcionamento do Conselho de Governo e da CREDEN estão contidas, respectivamente, na Lei nº 10.683/2003, e no Decreto nº 4.801/2003. O art. 6º da Lei nº 10.683/2003 estabelece ao GSI/PR, entre outras atribuições, a coordenação das atividades de segurança da informação.

A dimensão e a assimetria da APF representa importante desafio para a área de SIC e de SegCiber. Na atualidade, são 39 ministérios, cerca de seis mil entidades governamentais, mais de um milhão de servidores federais, em torno de 320 grandes redes do Governo Federal, mais de 16,5 mil sítios de governo que superam 12 milhões de páginas WEB, e uma crescente participação e controle social.

O GSI/PR, diante de tal desafio, instituiu em 2006, para trato das questões afetas à SIC e à SegCiber, o Departamento de Segurança da Informação e Comunicações (DSIC), com abrangência de atuação na APF, e três áreas finalísticas para o cumprimento de sua missão, a saber: Gestão de SIC, Centro de Tratamento de Incidentes de Redes da Administração Pública Federal - CTIR Gov, e Credenciamento de Segurança.

A área de Gestão de SIC executa o planejamento e a gestão orientada aos órgãos e entidades da APF, por meio de programas de conscientização e capacitação dos agentes públicos, do apoio à implementação dos requisitos metodológicos necessários de SIC, bem como pela difusão do arcabouço normativo de SIC e de SegCiber, visando o seu cumprimento. A área também é responsável pela gestão das reuniões do Comitê Gestor da Segurança da Informação (CGSI/CDN).

A área de tratamento de incidentes (CTIR Gov), com a missão precípua de coordenar e acompanhar o tratamento e a resposta aos incidentes em redes computacionais da APF, vem contribuindo para as soluções integradas e a geração de estatísticas de incidentes de segurança, além de apoiar a criação e o fortalecimento de equipes especializadas (ETIR) nos órgãos e entidades da APF, disseminando informações relativas a ameaças, vulnerabilidades e tendências de ataques cibernéticos, em colaboração com outras equipes no Brasil e exterior.

A área finalística do sistema de credenciamento, após a promulgação da LAI, foi reformulada e estabeleceu-se o Núcleo de Segurança e Credenciamento (NSC) como órgão central da cadeia de credenciamento no âmbito do Poder Executivo federal, com

o objetivo de promover e regular o tratamento da informação classificada em qualquer grau de sigilo. O NSC busca assegurar a manutenção da cadeia de confiança entre os entes, públicos e privados, que tratam informação classificada em qualquer grau de sigilo do Governo Federal, inclusive com organismos internacionais.

A Agência Brasileira de Inteligência (ABIN), órgão vinculado ao GSI/PR, conta em sua estrutura com o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC), criado em 1982 para sanar deficiência do Brasil em garantir o sigilo dos canais de comunicação dos órgãos estratégicos da Administração Pública Federal. Desde então, vem desenvolvendo soluções de segurança da informação e comunicações baseadas em algoritmos criptográficos de Estado, bem como executando trabalhos de pesquisa e desenvolvimento na área da segurança cibernética.

Assim, na última década, os temas de SIC e de SegCiber passaram a ser reconhecidos por vários atores do Governo Federal como relevantes e de competência e coordenação político estratégica de órgão da Presidência da República, com abrangência para a APF, incluídas ações de segurança das infraestruturas críticas da informação.

Diante deste cenário dinâmico, como forma de colaborar com panorama de fundo da Segurança da Informação e Comunicações e da Segurança Cibernética, no âmbito do Governo Federal, apresentam-se no capítulo “Marcos do Governo Brasileiro em SIC e SegCiber” alguns dos marcos legais, normativos e institucionais alcançados, distribuídos na linha de tempo que compreende o período de 2000 até o 1º trimestre de 2015, os quais realçam, para além das ações já empreendidas, a complexidade dos temas, a diversidade de atores, e a importância desta Estratégia.

Por fim, não se pode deixar de citar o “Plano Brasil 2022”, publicado em 2010 pela Secretaria de Estudos Estratégicos da Presidência da República (SAE), o qual representa um pensamento estratégico do futuro do País e fixa metas para o ano de 2022, momento em que o Brasil comemora o bicentenário de sua independência.

Cabe destacar, portanto, o alinhamento desta Estratégia ao citado “Plano Brasil 2022” bem como o seu efetivo apoio ao alcance das metas do centenário, dentre outras, as metas a seguir apresentadas: i) Economia: modernizar o funcionamento da administração pública; ii) Sociedade: universalizar o acesso aos bens e conteúdos culturais a todos os brasileiros; iii) Infraestrutura: assegurar acesso integral à banda larga, à velocidade de 100 Mbps, a todos os brasileiros; e, iv) Estado: garantir pleno exercício do direito de acesso a informações públicas e consolidar a Internet como um terreno de liberdade de expressão.

MARCOS DO GOVERNO BRASILEIRO EM SIC E SEGCIBER

PERÍODO: 2000 A 2015

Em 2000:

- Foi publicado o Decreto nº 3.505/2000, instituindo a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF). Esse Decreto criou o Comitê Gestor da Segurança da Informação (CGSI), com atribuição de assessorar a Secretaria-Executiva do Conselho de Defesa Nacional (CDN) na consecução das diretrizes da Política, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto. Integram o CGSI os seguintes 17 órgãos da APF: GSI/PR (que o coordena); CC/PR; CGU; AGU; SECOM/PR; SG/PR; MJ; MD; MRE; MF; MPS; MS; MDIC; MP; MC; MCTI; MME.

Em 2001:

- Foi publicada a Medida Provisória nº 2.200 de 28 de junho de 2001, instituindo a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), incluindo o GSI/PR como membro do Comitê Gestor da ICP-Brasil.
- Foi publicado o Decreto nº 3.872 de 18 de julho de 2001, que dispõe sobre o Comitê Gestor da Infra Estrutura de Chaves Públicas Brasileira (CG ICP-Brasil). Este Decreto foi revogado pelo Decreto nº 6.605/2008.
- Foi publicado o Decreto nº 3.996 de 31 de outubro de 2001, que dispõe sobre a prestação de serviços de certificação digital no âmbito da APF.

Em 2002:

- Foi publicado o Decreto nº 4.553 de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesses da segurança da sociedade e do Estado, no âmbito da APF. Esse Decreto foi revogado pelo Decreto nº 7.845/2012.

Em 2003:

- Lei nº 10.683, de 28 de maio de 2003, em seu art. 6º, estabelece ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) a competência de

coordenar as atividades de inteligência federal e de segurança da informação do governo, entre outras.

- Decreto nº 4.801, de 06 de agosto de 2003, cria a Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo, com a finalidade de formular políticas públicas e diretrizes de matérias relacionadas com a área das relações exteriores e defesa nacional do Governo Federal, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos, no âmbito de ações cujo escopo ultrapasse a competência de um único Ministério. Integravam à época os seguintes Ministérios: GSI/PR (que a preside); Casa Civil/PR; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente e Ciência e Tecnologia, sendo convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o Chefe do Estado-Maior Conjunto das Forças Armadas (composição atualizada em 2009 e 2013).
- Decreto nº 4.829, de 03 de setembro de 2003, que dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGI.br, sobre o modelo de governança da Internet no Brasil, e estabelece a coordenação do mesmo a ser exercida pelo, então, Ministério da Ciência e Tecnologia – MCT, contando com governança multissetorial, ou seja, participação de representantes do governo, da academia, do setor empresarial e do terceiro setor.

Em 2004:

- Criação da equipe de tratamento de incidentes em redes computacionais do governo, CTIR Gov, no GSI/PR;
- Lei nº 10.973, de 02 de dezembro de 2004, publicada como instrumento legal de fomento à inovação.

Em 2005:

- Foi realizada a “I Conferência de Segurança para o Governo (SECGOV-2005)”, sob a coordenação do GSI/PR, para tratar de temas atinentes à segurança da informação e comunicações.
- Em 13 de outubro o Brasil assina com Portugal, na Cidade do Porto, Acordo de Troca e Proteção Mútua de Informações Classificadas.
- Decreto nº 5.563, de 11 de outubro de 2005, regulamenta a Lei de Inovação (Lei nº 10.973/2004) que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo.

Em 2006:

- Decreto nº 5.772, de 08 de maio de 2006, dispõe sobre a reestruturação do GSI/PR, com inserção de novas atribuições relacionadas à Segurança da Informação no rol de competências da secretaria executiva. Fica, então, criado o Departamento de Segurança da Informação e Comunicações (DSIC), com a missão de planejar e coordenar as atividades de Segurança da Informação e Comunicações (SIC) na APF.
- Foi estabelecida a ação orçamentária 6232 (Capacitação de Recursos Humanos na Área de Segurança da Informação) destinada à formação e ao aprimoramento de recursos humanos com vistas à definição e à implementação de mecanismos capazes de fixar e fortalecer o desenvolvimento e a execução da Segurança da Informação.
- Foi estabelecida parceria do GSI/PR, como órgão coordenador das atividades de Segurança da Informação no Governo Federal, com vários órgãos, entre eles, o Ministério do Turismo (MTur), Controladoria-Geral da União (CGU), Advocacia-Geral da União (AGU), Secretaria da Receita Federal (SRF), Secretaria da Receita Previdenciária (SRP), Instituto Nacional do Seguro Social (INSS), Empresa Brasileira de Pesquisa Agropecuária (EMBRAPA), Serviço Federal de Processamento de Dados (SERPRO), Empresa Brasileira de Radiodifusão (Radiobrás), Agência Brasileira de Inteligência (ABIN), Banco Central do Brasil (BCB), Banco do Brasil (BB), Caixa Econômica Federal (CEF), Petróleo Brasileiro S.A. (Petrobrás) e a Rede Nacional de Ensino e Pesquisa (RNP), com a finalidade de organizarem atividades em conjunto que possibilitassem a disseminação da cultura da Segurança da Informação.
- Foi realizada a "II Conferência de Segurança para o Governo (SECGOV-2006)", já sob a coordenação do DSIC/GSI/PR.

Em 2007:

- Iniciou-se a primeira turma do "Curso de Especialização em Gestão de SIC (CEGSIC 2007-2008)", em convênio com o Departamento de Ciência da Computação da Universidade de Brasília. O CEGSIC 2007-2008 teve carga horária de 375 horas aula, realizadas em regime presencial, nas dependências da Universidade de Brasília. Contou com a participação de 40 alunos agentes públicos da APF e formou 36 especialistas.
- Foi realizado o "I Congresso de Segurança da Informação e Comunicações (SICGov-2008)", no Auditório do Anexo I do Palácio do Planalto, em Brasília, DF.
- Em 17 de setembro o Brasil assina com a Espanha, em Madri, Acordo de Troca e Proteção Mútua de Informações Classificadas.

Em 2008:

- Instrução Normativa GSI nº 01, publicada em 13 de junho de 2008, elaborada de forma colaborativa com os membros do Comitê Gestor de Segurança da Informação (CGSI), disciplinando a Gestão de Segurança da Informação e Comunicações na APF.
- Foram publicadas as primeiras Normas Complementares (NC) da IN 01 GSI/PR, a NC nº 01 sobre atividade de normatização e NC a nº 02 sobre metodologia de gestão de SIC.
- Acórdão 1.603/2008-TCU-Plenário de 13 de agosto, divulga o resultado do levantamento da governança de TI, realizado no processo do TCU nº 008.380/2007-1, e recomenda ao GSI/PR que oriente os órgãos e entidades da APF sobre a importância do gerenciamento da segurança da informação, promovendo, inclusive mediante orientação normativa, ações que objetive estabelecer e/ou aperfeiçoar a gestão da continuidade do negócio, a gestão de mudanças, a gestão de capacidade, a classificação da informação, a gerência de incidentes, a análise de riscos de TI, a área específica para gerenciamento da segurança da informação, a política de segurança da informação e os procedimentos de controle de acesso.
- Foi realizado o "II Congresso de Segurança da Informação e Comunicações (SICGov-2008)", no Auditório do Conjunto Cultural da Caixa Econômica Federal, em Brasília, DF.
- Decreto nº 6.703, de 18 de dezembro de 2008, aprova a Estratégia Nacional de Defesa (END) a qual estabelece o setor cibernético entre os 3 setores estratégicos do País, considerados essenciais para a defesa nacional. Realça que para o setor cibernético será constituída organização encarregada de desenvolver a capacitação cibernética nos campos industrial e militar. Além de realçar as medidas para a segurança das áreas de infraestruturas críticas, incluindo serviços, em especial no que se refere à energia, transporte, água e telecomunicações, a cargo dos Ministérios da Defesa, das Minas e Energia, dos Transportes, da Integração Nacional e das Comunicações, e ao trabalho de coordenação, avaliação, monitoramento e redução de riscos, desempenhado pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o que inclui as infraestruturas críticas de informação.
- Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação – SLTI, do Ministério do Planejamento, Orçamento e Gestão – MP, dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática – SISP, do Poder Executivo Federal.
- Em 13 de agosto, o Brasil assina com a Rússia, em Moscou, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
- Foi publicado o Decreto nº 6.605 de 14 de julho de 2008, dispondo sobre o Comitê Gestor da ICP-Brasil, revogando o Decreto nº 3.872/2001 e fazendo nova redação.

- Portaria GSI/PR nº 31, de 06 de outubro de 2008, institui a Rede Nacional de Excelência em Segurança da Informação e Criptografia – RENASIC.

Em 2009:

- Foram publicadas mais quatro Normas Complementares à IN 01 GSI/PR:

  ✓ NC 03/IN01/DSIC/GSI/PR - Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da APF;

  ✓ NC 04/IN01/DSIC/GSI/PR - Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal;

  ✓ NC 05/IN01/DSIC/GSI/PR - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal; e

  ✓ NC 06/IN01/DSIC/GSI/PR - Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

- Iniciou-se a segunda turma do "Curso de Especialização em Gestão de SIC (CEGSIC 2009-2010)", em convênio com o Departamento de Ciência da Computação da Universidade de Brasília. O CEGSIC 2009-2010 teve carga horária de 375 horas aula, realizadas em regime presencial, nas dependências da Universidade de Brasília. Contou com a participação de 40 alunos agentes públicos da APF e formou 39 especialistas.
- Foi realizado o "III Congresso de Segurança da Informação e Comunicações (SICGov-2009)", na Universidade Corporativa dos Correios, Brasília – DF, com foco em segurança cibernética.
- O DSIC/SE/GSI/PR apoiou o evento da Organização dos Estados Americanos (OEA), realizado nos dias 16 a 20 de novembro de 2009, no Rio de Janeiro, que contou com a presença de 136 participantes estrangeiros, representantes dos países do continente americano, com a finalidade de estabelecer proposta de "Estratégia Nacional de Segurança Cibernética do Hemisfério", para os países da região.
- Decreto nº 7.009, de 12 de novembro de 2009, inclui o tema segurança cibernética nos objetivos da Câmara de Relações Exteriores e Defesa Nacional – CREDEN do Conselho de Governo, e realça o acompanhamento e estudo de questões e fatos relevantes com potencial de risco à estabilidade institucional, para prover informações ao Presidente da República. A composição foi então atualizada contemplando os seguintes Ministérios: GSI/PR (que a preside); Casa Civil/PR; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; Ciência e Tecnologia; Fazenda e SAE/PR, sendo convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o

Chefe do Estado-Maior Conjunto das Forças Armadas (composição atualizada em 2013).

- Portaria CREDEN nº 45, de 8 de setembro de 2009, institui o Grupo Técnico de Segurança Cibernética, com o objetivo de propor diretrizes e estratégias para a Segurança Cibernética, no âmbito da Administração Pública Federal. Órgãos integrantes: GSI/PR; MRE; MJ; MD; MD/EB; MD/MB; e MD/COMAER.
- A Diretriz Ministerial nº 14/2009 atribuiu ao Exército Brasileiro institucionalizar o Núcleo do Centro de Defesa Cibernética do Exército (Nu CDCiber).

Em 2010:

- Foi contratada a Fundação Trompowsky do Exército Brasileiro para planejar, customizar e manter infraestrutura de ambiente virtual para a realização de Cursos de Fundamentos de Gestão de SIC, na modalidade de ensino a distância - EAD, incluindo a execução de duas turmas que, juntas, totalizaram 350 servidores de órgãos e entidades da APF.
- Iniciou-se a terceira turma do CEGSIC na modalidade de ensino a distância (EAD), em convênio com a Universidade de Brasília (UnB), destinado a especializar 180 servidores de órgãos e entidades da APF, formando 146 especialistas.
- Foi realizado o "IV Congresso de Segurança da Informação e Comunicações (SICGov-2010)", na Universidade Corporativa dos Correios, com o tema: Visão de Futuro para Segurança Cibernética.
- Foi publicado o Acórdão 2.308/2010-TCU-Plenário de 8 de setembro de 2010 divulgando o resultado do levantamento da governança de TI realizado no processo do TCU nº 000.390/2010-0. O referido Acórdão descreve que não houve melhora nos processos de segurança da informação na APF, porém, ressalva que a piora em parte dos indicadores pode não refletir deterioração da situação segurança da informação da APF, mas sim uma possível melhora na compreensão dos conceitos questionados, e por fim, reconhece o trabalho do GSI/PR a respeito da Segurança da Informação com a publicação da IN 01 GSI/PR e respectivas Normas Complementares.
- Foram publicadas mais 3 Normas Complementares à IN 01 GSI/PR:

  ✓ NC 07/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

  ✓ NC 08/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal; e

  ✓ NC 09/IN01/DSIC/GSI/PR - Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.

- Foi ativado o Núcleo do Centro de Defesa Cibernética, tendo como principal atribuição coordenar as atividades do setor cibernético no Exército.
- Em 22 de novembro, o Brasil assina com a Itália, em Roma, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
- Em 24 de novembro, o Brasil assina com Israel, em Tel Aviv, o Acordo de Troca e Proteção Mútua de Informações Classificadas.

Em 2011:

- Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) traz a primazia da transparência das informações sob a custódia do Estado.
- Decreto nº 7.579, de 11 de outubro de 2011, dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal, e estabelece que o Órgão Central do SISP, Ministério de Planejamento, Orçamento e Gestão, elaborará, em conjunto com os Órgãos Setoriais e Seccionais do SISP, a "Estratégia Geral de Tecnologia da Informação – EGTI" para a Administração direta, autárquica e fundacional do Poder Executivo Federal, revisada e publicada anualmente, para servir de subsídio à elaboração dos PDTI pelos órgãos e entidades integrantes do SISP.
- Foi publicado o Acórdão 1.145/2011-TCU-Plenário de 4 de maio de 2011, realizado no processo TCU nº 028.772/2010-5, especificando que o GSI/PR, dentre outros, é um Órgão Governante Superior (OGS) com a responsabilidade de normatizar aspectos da Segurança da Informação e Comunicações, em seus respectivos segmentos da APF.
- Transferência da Rede Nacional de Excelência em Segurança da Informação e Criptografia – RENASIC do GSI/PR para o CDCiber/EB/MD.

Em 2012:

- Foi publicado o Acórdão 1.233/2012-TCU-Plenário de 23 de maio de 2012 referenciando o resultado do levantamento da governança de TI realizado no processo do TCU nº 011.772/2010-7. O referido Acórdão recomenda ao GSI/PR que:

  ✓ Articule-se com as Escolas de Governo, notadamente à ENAP, a fim de ampliar a oferta de ações de capacitação em segurança da informação para os entes sob sua jurisdição;

  ✓ Oriente os órgãos e entidades sob sua jurisdição que a implantação dos controles gerais de segurança da informação positivados nas normas do GSI/PR não é faculdade, mas obrigação da Alta Administração, e sua não implantação sem justificativa é passível da sanção prevista na Lei; e

✓ Reveja a Norma Complementar 4/IN01/DSIC/GSIPR, uma vez que aborda o tema gestão de riscos considerando apenas ativo de informação e não ativo em sentido amplo, como o faz a NBR ISO/IEC 27.002 no item 7.1.1.

- Foram publicadas mais sete Normas Complementares à IN 01 GSI/PR:

✓ NC 10/IN01/DSIC/GSI/PR - Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

✓ NC 11/IN01/DSIC/GSI/PR - Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

✓ NC 12/IN01/DSIC/GSI/PR - Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

✓ NC 13/IN01/DSIC/GSI/PR - Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

✓ NC 14/IN01/DSIC/GSIPR - Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

✓ NC 15/IN01/DSIC/GSI/PR - Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta; e

✓ NC 16/IN01/DSIC/GSIPR - Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.

- Foi publicado o Acórdão 2.585/2012-TCU-Plenário de 26 de setembro de 2012 divulgando o resultado do levantamento da governança de TI realizado no processo do TCU nº 007.887/2012-4.
- O Decreto nº 7.724, de 16 de maio de 2012 regulamenta a LAI no âmbito do Poder Executivo Federal, estabelecendo as diretrizes para a transparência ativa e passiva. No mesmo dia, a Lei de Acesso à Informação entra em vigor.
- O Decreto nº 7.845, de 14 de novembro de 2012 é publicado encerrando a regulamentação da LAI, estabelecendo o tratamento para as informações com restrição de acesso e dispondo sobre o Núcleo de Segurança e Credenciamento (NSC) no GSI/PR.
- Foram publicadas duas leis contra o crime cibernético:

✓ Lei nº 12.737, de 30 de novembro de 2012, a qual dispõe sobre a tipificação criminal de delitos informáticos.

✓ Lei nº 12.735, de 30 de novembro de 2012, a qual tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares.

- A "Política Cibernética de Defesa" é estabelecida por meio da Portaria Normativa nº 3.389/MD, com a finalidade de orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos.

Em 2013:

- Foram publicadas mais duas Normas Complementares à IN 01 GSI/PR:

✓ NC 17/IN01/DSIC/GSI/PR - Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

✓ NC 18/IN01/DSIC/GSI/PR - Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

- Com a publicação da LAI em 2011 e seus Decretos regulamentadores no âmbito do Poder Executivo Federal, fez-se necessário revisar a NC 09/IN01/DSIC/GSI/PR, principalmente, em relação ao conceito de algoritmo de Estado.
- Conforme determinação do Acórdão nº 1.233/2012-TCU-Plenário de 23 de maio de 2012, foi feita a primeira revisão da NC 04/IN01/DSIC/GSI/PR, na qual foi incluído item 2, nas considerações gerais, o seguinte texto:

✓ A Gestão de Riscos de Segurança da Informação e Comunicações, objeto desta Norma Complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme definido nesta Norma.

- Iniciou-se a quarta turma do CEGSIC na modalidade de ensino a distância (EAD), em convênio com a Universidade de Brasília (UnB), destinado a especializar 216 servidores de órgãos e entidades da APF, com previsão de formatura de mais 140 especialistas ao final do curso em 2015.
- Portaria SAE/PR nº 124 institui Grupo de Trabalho Interministerial (GTI) com o objetivo de elaborar proposta de Plano Estratégico para promover ou subsidiar o aperfeiçoamento das políticas públicas voltadas à segurança e defesa do espaço cibernético nacional. O art. 3º da citada Portaria nomeia os membros Titulares e Suplentes que representam os seguintes órgãos que integram o GTI: SAE/PR; MD;

MRE; MEC; MDIC; MP; MCTI; MC; GSI/PR; CGI.br; ANATEL; SERPRO; DATAPREV; e TELEBRÁS.

- IN GSI/PR 02, de 5 de fevereiro de 2013, regulando o Credenciamento de Segurança e o tratamento de informação classificada em grau de sigilo.
- IN GSI/PR 03, de 6 de março de 2013, estabelecendo os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado.
- NC 01/IN02/DSIC/GSI/PR, de 27 de junho de 2013, inaugura os trabalhos de Credenciamento sob a égide das novas regras para o tratamento das informações classificadas em grau de sigilo.
- Decreto nº 8.096, de 04 de setembro de 2013, atualiza a composição da CREDEN, e a Câmara passa a contar com os seguintes Ministérios: GSI/PR (que a preside); Casa Civil/PR; Justiça; Defesa; Relações Exteriores; Planejamento, Orçamento e Gestão; Meio Ambiente; Ciência e Tecnologia; Fazenda; SAE/PR; Integração Nacional; Minas e Energia; e Transportes, sendo convidados a participar das reuniões, em caráter permanente, os Comandantes da Marinha, do Exército, da Aeronáutica e o Chefe do Estado-Maior Conjunto das Forças Armadas.
- Decreto Legislativo nº 3703, de 12 de julho de 2013, atualiza a "Estratégia Nacional de Defesa" e aprova o "Livro Branco de Defesa Nacional". Entre as premissas sobre o setor cibernético, cita que a proteção do espaço cibernético abrange um grande número de áreas, como: capacitação, inteligência, pesquisa científica, doutrina, preparo e emprego operacional; e gestão de pessoal.
- Decreto nº 8.135, de 04 de novembro de 2013, dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

Em 2014:

- A NC 09/IN01/DSIC/GSI/PR recebeu a segunda revisão, destacando-se o novo conceito de algoritmo registrado:

  ✓ Algoritmo Registrado: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processo sejam passíveis de controle e auditoria.

- A NC 07/IN01/DSIC/GSI/PR recebeu a primeira revisão, sendo incorporado o tema "Biometria" como controle de acesso.
- Foram publicadas três normas complementares à IN 01 GSI/PR:

✓ NC 19/IN01/DSIC/GSI/PR estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta;

✓ NC 20/IN01/DSIC/GSI/PR estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta; e

- NC 21/IN01/DSIC/GSI/PR estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. No mesmo ano, essa NC recebeu a primeira revisão.

- Foi publicado o Acórdão 3.051/2014-TCU-Plenário de 5 de novembro de 2014, referente ao processo do TCU nº 023.050/2013-6. Esse Acórdão contextualiza as auditorias realizadas em diversos órgãos e entidades da Administração Pública federal com o objetivo de avaliar a implementação dos controles de TI informados em resposta ao levantamento do perfil de governança de TI de 2012. Pontos de interesses da segurança da informação:

✓ A segurança da informação segue sendo objeto de preocupação. Há baixa conformidade das organizações para com os normativos e com as boas práticas aplicáveis. Na maioria das organizações fiscalizadas na primeira fase, falhas foram observadas: a) 80% - falhas na gestão de continuidade de negócio; b) 70% - falhas no controle de acesso; c) 75% - falhas na gestão de incidentes; e, d) 85% - falhas na gestão de riscos de segurança da informação.

✓ Principais causas estão ligadas a falhas típicas de governança, como a falta de designação de um responsável pela segurança da informação, fato observado em 40% das organizações.

✓ Houve tendência de mudança de comportamento dos dirigentes públicos sobre a segurança da informação.

✓ A redução dos percentuais observados não se traduz necessariamente em retrocesso, mas pode ser interpretado como amadurecimento dos gestores de TI no sentido de compreender melhor os conceitos relacionados à segurança da informação.

✓ Ainda não há, por exemplo, um planejamento estratégico do Estado brasileiro que reúna e coordene ações dos diversos atores responsáveis por assuntos ligados a essa área.

✓ Recomendações ao GSI/PR: elabore e acompanhe periodicamente planejamento que abranja a estratégia geral de segurança da informação para o setor sob sua jurisdição; e alerte as organizações sob sua jurisdição que a elaboração periódica de planejamento das ações de segurança da informação é obrigação expressa prevista no item 3.1 da Norma Complementar 02/IN01/DSIC/GSI/PR.

- Foi publicado o Acórdão 3.117/2014-TCU-Plenário de 12 de novembro de 2014, referente ao processo do TCU nº 003.732/2014-2. Trata-se de relatório de levantamento realizado com o objetivo de acompanhar a situação da Governança de Tecnologia da Informação na Administração Pública Federal, realizado a cada dois anos pelo TCU. Pontos de interesses da segurança da informação:

  - ✓ A segurança da informação tem sido objeto de preocupação em todos os levantamentos anteriores por causa da baixa conformidade das organizações em relação aos normativos e às boas práticas aplicáveis.
  - ✓ Como referência para elaboração das questões da auditoria, foram utilizadas principalmente a norma técnica ABNT NBR ISO/IEC 27002:2005 e as normas complementares do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI/PR).
  - ✓ Apesar de ser o principal instrumento direcionador da gestão da segurança da informação, preocupa que apenas 66% (15% parcialmente e 51% integralmente) das organizações participantes declarem dispor de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.
  - ✓ Apesar de ser o principal instrumento direcionador da gestão da segurança da informação, preocupa que apenas 66% das organizações participantes declarem dispor de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório;
  - ✓ O comitê de segurança da informação formalmente instituído, composto por representes das áreas relevantes da organização e responsável por formular e conduzir diretrizes para a segurança da informação corporativa, é encontrado em 62% das organizações, segundo declarado.
  - ✓ Observa-se que apenas 50% das organizações declararam possuir gestor da segurança da informação formalmente designado, responsável pelas ações corporativas de segurança da informação.
  - ✓ Quanto à política que normatiza o acesso às informações e aos recursos e serviços de TI, somente 52% (declararam dispor desse normativo formalmente instituído, com cumprimento obrigatório).
  - ✓ Quanto à política de cópias de segurança (backup), que são necessárias para garantir a disponibilidade das informações em casos de falhas de sistemas ou pessoas, somente 54% declararam dispor desse normativo formalmente instituído, com cumprimento obrigatório.

- Lei nº 12.965, de 23 de abrul de 2014, conhecida como Marco Civil da Internet, estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
- Portaria Normativa MD 2.777, de 27 de outubro de 2014, aprova a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e cria o Comando de Defesa Cibernética – ComDCiber e a Escola Nacional de Defesa

Cibernética – EnaDCiber, na Estrutura Regimental do Comando do Exército, com ênfase na implantação e a consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, o apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética, bem como a criação do Observatório de Defesa Cibernética.

- Em 14 de abril o Brasil assina com a Suécia, em Estocolmo, o Acordo de Troca e Proteção Mútua de Informações Classificadas.
- Durante todo o ano, na qualidade de Autoridade Nacional de Segurança (ANS), exercida GSI/PR, manteve estreita relação com o Ministério das Relações Exteriores na articulação, tanto de ajustes nos Acordos de Troca e Proteção Mútua de Informações Classificadas assinados com seis países, visando alinhamento à LAI, quanto de novos acordos demandados por outros 14 países.
- Portaria Interministerial MP MD MC nº 141, de 02 de maio de 2014, regulamenta o Decreto nº 8.135/2013, dispõe para toda a administração pública federal o dever de realizar as suas comunicações, armazenamentos e recuperações de dados através de redes de telecomunicações e serviços de tecnologia de informação fornecidos por órgãos ou entidades da própria administração pública federal (SERPRO, TELEBRÁS, DATAPREV, entre outros), com exceção de serviço móvel pessoal e serviço telefônico fixo comutado, garantindo-se a segurança da informação e comunicações conforme normativos do GSI/PR. O SERPRO inicia implantação do serviço de mensageria Expresso V3 na APF.
- Publicada a "Doutrina Militar de Defesa Cibernética (MD31-M-07, 1ª Edição/2014)", por meio da Portaria normativa nº 3.010/MD, de 18 de novembro de 2014.
- Relatório Final da CPI da Espionagem, elaborado pela Comissão Parlamentar de Inquérito destinada a investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos, com o objetivo de monitorar e-mails, ligações telefônicas, dados digitais, além de outras formas de captar informações privilegiadas ou protegidas pela Constituição Federal aponta para diversos aspectos essenciais e recomendações à segurança da informação e segurança cibernética, entre eles:

✓ Elaboração de uma Estratégia Nacional de Segurança Cibernética, realçando que houve unanimidade entre os convidados à CPI, de que mais urgente do que a Estratégia, é que sejam delineadas as principais medidas de segurança cibernética para o Estado brasileiro, englobando ações coordenadas entre os setores público e privado.

✓ Criação de uma agência para a segurança cibernética no âmbito da Administração Pública Federal, favorecendo visão de conjunto no tema e ações mais eficazes e efetivas. Alternativamente à criação de um novo órgão, poderia ser alterada a estrutura de órgão já existente, modificando suas atribuições, para lhe conferir capacidade de atuar, com independência, em sua totalidade e em estreita

coordenação com os demais órgãos atuantes nos mais diversos temas que englobam a segurança cibernética.

Até o 1º. Trimestre de 2015

- Regulamentação do Marco Civil da Internet, processo de regulamentação da Lei nº 12.965/2014, em andamento por meio de consultas públicas pelo Comitê Gestor da Internet e pelo Ministério da Justiça.
- Projeto de Lei de Dados Pessoais. Em consulta pública disponibilizada pelo Ministério da Justiça
- Alteração da Instrução Normativa SLTI nº 04, em 12 de janeiro de 2015, estabelecendo a "Estratégia Geral de Tecnologia da Informação e Comunicações (EGTIC) – 2014/2015", a qual compreende um instrumento de gestão do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), traçando a direção da Tecnologia da Informação e Comunicações (TIC), e definindo o plano estratégico que visa promover a melhoria contínua da gestão e governança de TIC no governo.
- Em fevereiro de 2015, realização da "II Jornada de Discussões dos Projetos ENaDCiber e SHCDCiber", evento organizado pelo CDCiber/EB/MD em parceria com a UnB, para debater sobre a concepção e a viabilidade de criação da Escola Nacional de Defesa Cibernética (ENaDCiber) e do Sistema de Homologação e Certificação de Produtos e Serviços de Defesa Cibernética (SHCDCiber).
- Decreto nº 8.414, de 26 de fevereiro de 2015, institui o Programa "Bem Mais Simples Brasil" com a finalidade de simplificar e agilizar a prestação dos serviços públicos e de melhorar o ambiente de negócios e a eficiência da gestão pública. Objetivos: (i) simplificar e agilizar o acesso do cidadão, das empresas e das entidades sem fins lucrativos aos serviços e informações públicos; (ii) promover a prestação de informações e serviços públicos por meio eletrônico; (iii) reduzir formalidades e exigências na prestação de serviços públicos; (iv) promover a integração dos sistemas de informação pelos órgãos públicos para oferta de serviços públicos; (v) celebrar o "Pacto Bem Mais Simples Brasil" com os demais Poderes da União e com os Estados, o Distrito Federal e os Municípios; e (vi) modernizar a gestão interna da administração pública.

FINALIDADE E APLICAÇÃO

A SIC e a SegCiber, base da Defesa Cibernética, visam assegurar o uso do espaço cibernético, impedindo ou dificultando, em seu âmbito, ações contra os interesses do País e da sociedade (Figura 1).

Assim, a presente "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal – 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008, coordenada e integrada pelo Gabinete de Segurança Institucional da Presidência da República – GSI/PR, tem a finalidade de apresentar as diretrizes estratégicas para o planejamento de segurança da informação e comunicações e de segurança cibernética no âmbito da APF, objetivando a articulação e a coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais encontram-se expostas as organizações e a sociedade.

As diretrizes dessa Estratégia aplicam-se a todos os órgãos e entidades que integram a APF.

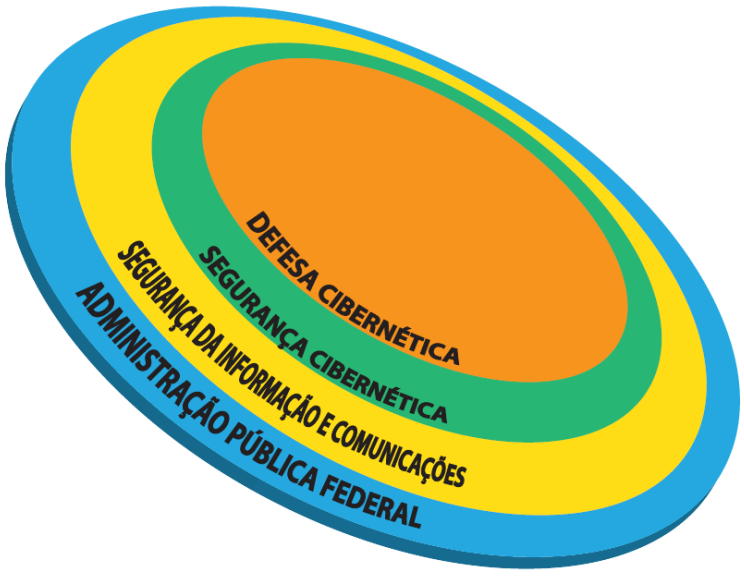


Figura 1 – Visão em Camadas: SIC, SegCiber e Defesa Cibernética

METODOLOGIA

A elaboração dessa "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal" utilizou, com adaptações, a consagrada metodologia de planejamento e gestão estratégica denominada *Balanced Scorecard* (BSC), proposta por Robert Kaplan e David Norton.

O valor dessa metodologia reside na capacidade de traduzir a visão e a estratégia em ações que de fato contribuam para o alcance dos objetivos estratégicos, além de prover um sistema de retroalimentação que permite o ajuste e o aprimoramento contínuo por meio do acompanhamento de indicadores e metas, englobando inclusive os princípios do PDCA.

A partir de adaptações da metodologia BSC ao ambiente governamental, no contexto da SIC e da SegCiber, foram consideradas quatro perspectivas basilares sobre as quais foram construídos os objetivos estratégicos e as metas: (i) Orçamentária; (ii) Aprendizagem, Crescimento e Inovação; (iii) Governo; e (iv) Resultados para a Sociedade.

A perspectiva Orçamentária tem natureza estruturante e diz respeito ao aporte contínuo e adequado de recursos do orçamento federal para que se viabilize as ações necessárias ao alcance dos objetivos propostos nessa Estratégia.

A perspectiva Aprendizagem, Conhecimento e Inovação, que também tem natureza estruturante, envolve o investimento em capital humano, abrangendo ações de sensibilização, conscientização, treinamento, capacitação e especialização nas áreas de SIC e de SegCiber, como forma de preparar os agentes públicos para promover mudanças e viabilizar a consecução dos objetivos propostos na Estratégia.

Por sua vez, a perspectiva Governo engloba os processos internos, a legislação, as articulações, as competências institucionais, as estruturas governamentais e tudo o mais que envolva as intra e inter-relações da APF com os demais atores, no alcance dos objetivos.

Por fim, a perspectiva Resultados para a Sociedade representa a finalidade precípua da ação Estatal – a de direcionar sua conduta sempre visando os interesses e demandas sociais, e engloba as ações em SIC e SegCiber que resultem em benefícios para a sociedade, tais como proteção da privacidade, transparência, democratização do acesso a informação e salvaguarda dos ativos de informação sigilosos.

Tendo em vista a natureza transversal dos Objetivos Estratégicos de SIC e de SegCiber, as metas foram construídas a partir de uma visão holística, ou seja, considerando a Estratégia como um todo, não se vinculando necessariamente cada meta a um único objetivo estratégico.

Para a elaboração da minuta da Estratégia foi nomeado um Grupo Técnico formado por servidores do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República – GSI/PR, órgão com a atribuição de planejar e coordenar a segurança da informação no âmbito da APF, conforme prevê a Lei nº 10.683/2003 e o regramento infralegal.

A iniciativa apoiou-se ainda na jurisprudência do Tribunal de Contas da União, em especial no Acórdão 1.145/2011 do Plenário, especificando que o GSI/PR, dentre outros, é um Órgão Governante Superior (OGS) o qual tem a responsabilidade de normatizar e fiscalizar os aspectos da Segurança da Informação e Comunicações, em seus respectivos segmentos da Administração Pública Federal; e no Acórdão 3.051/2014 do Plenário, que concluiu competir ao GSI, no âmbito do Poder Executivo, "*o papel de promover o desenvolvimento de uma estratégia para melhoria da segurança da informação [...], ainda que o faça em articulação com outros órgãos no âmbito das respectivas competências*".

Objetivando a articulação e a colaboração dos demais órgãos e entidades da APF, o GSI/PR consultou o Comitê Gestor de Segurança da Informação (CGSI) – instância de assessoramento criada por meio do Decreto nº 3.505/2000 no âmbito do Conselho de Defesa Nacional (CDN), cuja coordenação cabe ao GSI/PR e da qual fazem parte dezessete órgãos da APF –, como forma de buscar o alinhamento com os diversos atores, a efetividade dos objetivos propostos e o aprimoramento das diretrizes da Estratégia.

REFERENCIAL ESTRATÉGICO

MISSÃO DA ESTRATÉGIA

Fortalecer a política e o planejamento de segurança da informação e comunicações e de segurança cibernética na Administração Pública Federal, visando assegurar e defender os interesses do Estado e da sociedade para a preservação da soberania nacional.

VISÃO DE FUTURO DA ESTRATÉGIA

Ser reconhecida como instrumento de planejamento governamental para a excelência em segurança da informação e comunicações e em segurança cibernética na Administração Pública Federal.

VALORES DA ESTRATÉGIA

Ética: Ter como padrão de conduta ações que busquem a verdade dos fatos, amparadas em honestidade, moralidade, respeito, coerência e probidade na administração pública.
Colaboração: Atuar com dedicação, empenho e envolvimento em permanente colaboração e comunicação com os órgãos e entidades da APF, mantendo diálogos contínuos com os demais atores atuantes nas áreas de SIC e de SegCiber no país e exterior.
Efetividade: Atendimento às demandas da sociedade nas áreas de SIC e de SegCiber, por intermédio da APF, com foco em resultados.
Disseminação da cultura de SIC e de SegCiber: Promover o comprometimento da sociedade com os valores, visões, boas práticas, símbolos, hábitos, comportamentos e políticas, relativas à segurança da informação e comunicações e à segurança cibernética.
Inovação: Propor e implementar soluções criativas, novas ou adaptadas, no âmbito da SIC e da SegCiber, sempre na vanguarda da ciência e tecnologia.
Liderança: Atuar com liberdade e autonomia de forma técnica, proativa,

competente, responsável, imparcial, coerente e objetiva e estar comprometido com a missão institucional, com a capacidade de influenciar e mobilizar os diversos órgãos e entidades da APF para a consecução dos objetivos de SIC e de SegCiber, em prol da sociedade.
Apoio às Políticas Públicas: Priorizar as ações, programas e atividades desenvolvidas pelo Estado, no âmbito da SIC e da SegCiber, que correspondam a direitos assegurados constitucionalmente ou que se afirmam pelo reconhecimento das demandas da sociedade.

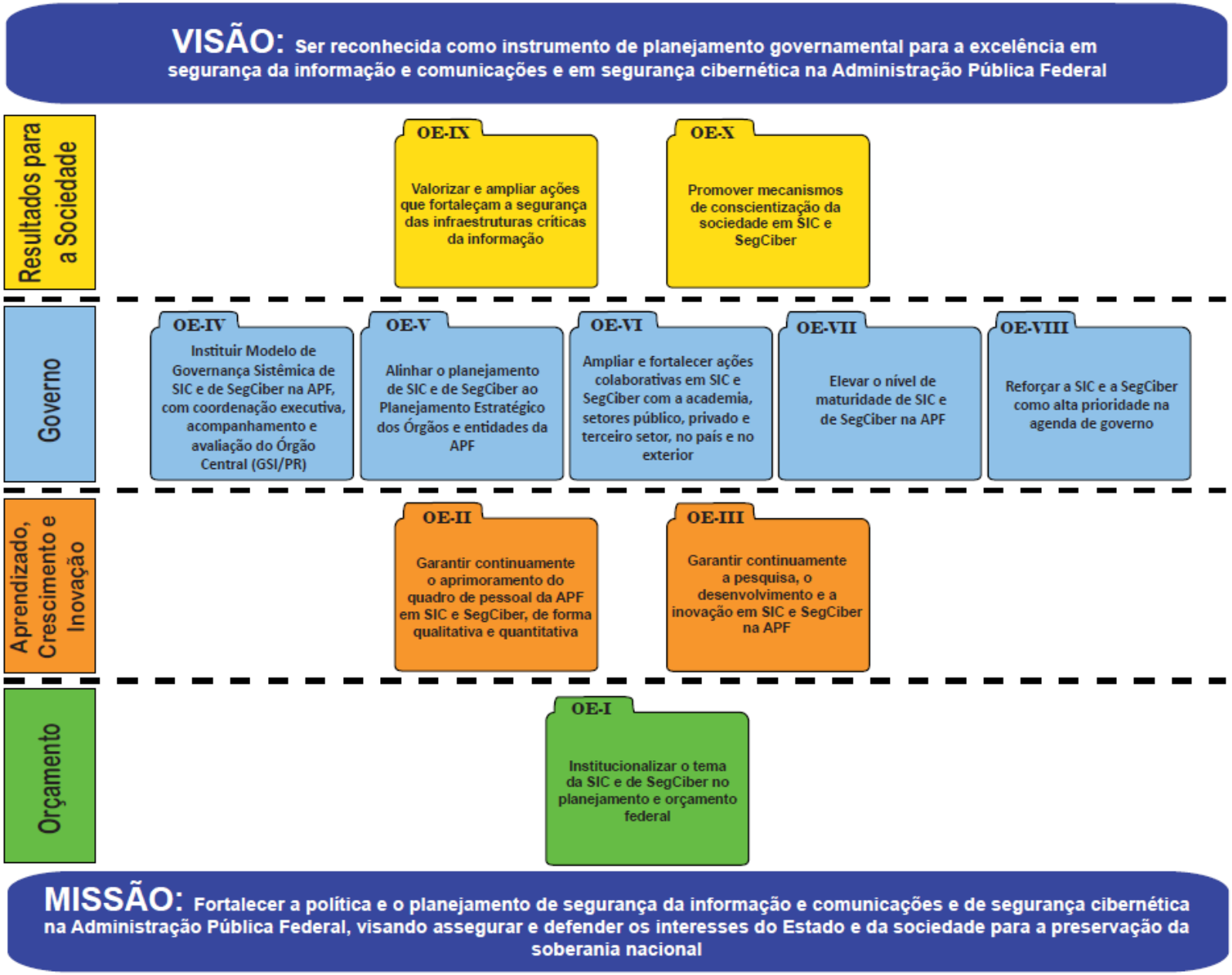
PRINCÍPIOS NORTEADORES DA ESTRATÉGIA

Órgão Central: contribuir com o estabelecimento de um órgão central e de um sistema nacional, objetivando a coordenação executiva, o acompanhamento e a avaliação da implantação e execução da Política Nacional de SIC e SegCiber.
Governança: contribuir com a definição de um modelo de governança sistêmica de SIC e de SegCiber, de amplo alcance e cobertura para uma conexão forte entre os múltiplos atores, em nível nacional.
Política Nacional: contribuir com a formulação da Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética.
Capacidade de posicionamento e de respostas da Nação: contribuir com a criação de uma robusta capacidade de posicionamento e de respostas da Nação frente às potenciais quebras de segurança e ameaças cibernéticas, fortalecendo a alocação de recursos financeiros, tecnológicos e humanos.
Comprometimento da Alta Administração: envolver a Alta Administração dos órgãos e entidades da Administração Pública Federal em relação às diretrizes e ações de SIC e de SegCiber no âmbito de suas atuações.
Marcos Legais: colaborar para o aprimoramento e atualização dos marcos legais em SIC e SegCiber.
Articulação e Parcerias: garantir que a SIC e a SegCiber estejam contempladas em termos, acordos, contratos e instrumentos firmados entre a APF e setores públicos ou privados, nacionais ou internacionais.
Soberania Nacional: reconhecer as áreas de SIC e de SegCiber como estratégicas para a soberania nacional, garantindo recursos contínuos e adequados.
Cooperação: promover a cooperação nacional e internacional, visando trocas de experiências e o fortalecimento dos temas de SIC e de SegCiber no âmbito da APF e com setor produtivo e academia.
Integração: fomentar e fortalecer ações conjuntas visando à integração entre as áreas de SIC e de SegCiber com outras áreas que atuam no espaço cibernético.
Resiliência: contribuir com o aumento da capacidade de resiliência dos ativos de informação e das infraestruturas críticas.

MAPA ESTRATÉGICO

O Mapa Estratégico segue uma abordagem em perspectivas, criando uma relação de causa e efeito e explicitando um caminho para se chegar aos resultados almejados. Ou seja, no caso presente, é preciso assegurar recursos suficientes no orçamento – motivo pelo qual a perspectiva orçamentária encontra-se na base do processo – de forma que se invista em aprendizagem, capacitação e inovação, dando condições para que os atores de Governo envolvidos promovam as melhorias necessárias nas instituições, nas estruturas e nos processos da gestão governamental e das políticas públicas, derivando na entrega de resultados efetivos para a sociedade e na melhoria do próprio Estado.

MAPA ESTRATÉGICO



OBJETIVOS ESTRATÉGICOS

Os objetivos estratégicos desta "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal" representam forças motrizes para o cumprimento da missão e o alcance da visão de futuro da mesma, e foram alinhados, também, aos princípios norteadores e valores, ora propostos.

Espera-se que tais objetivos estratégicos, além de alcançar os resultados da Estratégia, fomentem, no âmbito da APF e em futuro breve, o estabelecimento da Governança Sistêmica de SIC e de SegCiber, com vistas à institucionalização e ao fortalecimento da gestão pública de tais áreas na esfera do Poder Executivo federal e oportunamente em nível nacional. Tal visão sistêmica deve basear-se num modelo que reúna tanto a sociedade civil quanto os entes federativos da República – União, estados, municípios e Distrito Federal – com seus respectivos Sistemas de SIC e de SegCiber, organizados de forma autônoma e em regime de colaboração.

À semelhança de outros, esses sistemas de SIC e de SegCiber estabelecerão efetiva articulação entre Estado e sociedade, fortalecendo a organicidade, a racionalidade, a efetividade, os investimentos, a inovação e a estabilidade das políticas públicas de SIC e de SegCiber, definidas como de Estado.

A SIC e a SegCiber são estratégicas para a Nação, cabendo à APF direcionar esforços para a consecução dos objetivos propostos nesta Estratégia, conforme apresentados a seguir.

OE-I INSTITUCIONALIZAR O TEMA DE SIC E DE SEGCIBER NO PLANEJAMENTO E ORÇAMENTO FEDERAL.

A importância estratégica para o país dos temas de SIC e de SegCiber, conforme já contextualizado, exige um tratamento apropriado e prioritário por parte da Alta Administração da APF, que esteja à altura dos desafios atuais.

A institucionalização desses temas nos instrumentos de planejamento e orçamento do Governo é fundamental para que tais áreas avancem e sejam vistas no nível estratégico requerido, conquistando destaque no planejamento, bem como aportes contínuos e adequados de recursos do orçamento federal.

Considerando que o Plano Plurianual (PPA), instituído na Constituição Federal de 1988, tem a finalidade de ser um instrumento de planejamento e gestão estratégica do Governo Federal, e caracteriza-se como principal instrumento orientador das peças orçamentárias, realça-se o necessário estabelecimento de programas no PPA – e, como meta, no PPA 2016-2019 – que englobem as temáticas de SIC e de SegCiber e que permitam uma abordagem transversal e multissetorial das políticas públicas, passo importante para o atingimento dos objetivos propostos nessa Estratégia.

Certamente, há que se definir, com base em amplos debates com atores chave do governo, da academia, do setor privado e do terceiro setor, percentual do PIB a ser formalizado como patamar mínimo de investimento em SIC e em SegCiber, de forma a estabelecer um ciclo virtuoso de desenvolvimento em prol da soberania nacional e da segurança institucional como um todo.

Para além das dimensões estratégica e tática abordadas no PPA, é fundamental que os órgãos busquem a adequada operacionalização das ações de SIC e de SegCiber estabelecidas na esfera orçamentária (LOA), no âmbito de suas respectivas áreas de atuação, por meio do adequado alinhamento entre o planejamento de SIC e de SegCiber e o Planejamento Estratégico Institucional dos órgãos e entidades da APF, em conformidade com a Instrução Normativa GSI/PR nº 01/2008 e suas respectivas Normas Complementares, em especial a Norma Complementar nº 02/IN01/DSIC/GSIPR.

OE-II GARANTIR CONTINUAMENTE O APRIMORAMENTO DO QUADRO DE PESSOAL DA APF EM SIC E SEGCIBER, DE FORMA QUALITATIVA E QUANTITATIVA.

Os profissionais atuantes em SIC e SegCiber na APF, face a sua atuação relevante, somadas as responsabilidades já estabelecidas no arcabouço normativo do GSI/PR, devem ser valorizados quali e quantitativamente, amparado, dentre outros, nas diretrizes da Política Nacional de Desenvolvimento de Pessoal da APF (Decreto nº 5.707/2006).

Orienta-se, desta forma, que os órgãos e entidades da APF estabeleçam, em seus respectivos planejamentos de SIC e de SegCiber, programas de desenvolvimento de habilidades, aperfeiçoamento e atualização profissional com recursos adequados à demanda institucional, de forma a promover aprimoramento contínuo no curto, médio e longo prazo, em consonância com as normas complementares NC nº 17/IN01/DSIC/GSI/PR e NC nº 18/IN01/DSIC/GSI/PR.

Cabe ainda estimular parcerias com Escolas de Governo, bem como com outras instituições, universidades e empresas, no sentido de desenvolver programas de ensino, em todos os níveis, voltados à formação e ao aprimoramento de recursos humanos nas áreas de SIC e de SegCiber. Tais ações visam atender as demandas de sensibilização, conscientização, capacitação e especialização, de modo a fomentar o aperfeiçoamento contínuo e a permanência de tais profissionais, e contribuir com a robustez da Governança Sistêmica de SIC e de SegCiber da APF.

O estudo de viabilidade da criação de uma carreira de Estado em SIC e SegCiber, para atuação desses profissionais junto à Alta Administração, considerando que as áreas são críticas, exclusivas de Estado, de elevada sensibilidade, altamente estratégicas e preponderantes à preservação da soberania nacional, constitui importante fator para melhor consecução desse objetivo estratégico.

Salienta-se que é obrigatório para os órgãos e entidades da APF a nomeação de seus gestores de SIC, dos responsáveis pelas ETIR, dentre outros, com responsabilidades bem definidas, e exclusivas para a atuação de servidores de carreira civis (regidos pela Lei nº 8.112/1990) e militares (Lei 6.880/1980), a despeito da criação do necessário plano de carreira, cargos e salários na APF.

Em suma, a valorização dos profissionais atuantes nas áreas de SIC e de SegCiber proporciona uma contínua elevação do nível de maturidade das áreas na APF. Ademais, o aporte contínuo de investimento na formação e aperfeiçoamento desses profissionais contribui com a eficiência e efetividade, bem como com a formação de massa crítica e a disseminação da cultura de SIC e de SegCiber na sociedade brasileira.

OE-III GARANTIR CONTINUAMENTE A PESQUISA, O DESENVOLVIMENTO E A INOVAÇÃO EM SIC E SEGCIBER NA APF.

Face aos desafios atuais em nível global, bem como diante das ameaças e oportunidades já contextualizados anteriormente, o fortalecimento e a priorização das áreas de SIC e de SegCiber, na ciência; na pesquisa básica e aplicada; no desenvolvimento de tecnologias e de metodologias; e na inovação devem ser permanentemente articulados com atores chave de fomento do Governo Federal, em especial com o Ministério da Ciência, Tecnologia e Inovação (MCTI), visando à geração de conhecimentos e à agregação de valor em produtos, serviços e tecnologias de tais áreas, e respectivos setores produtivos.

Outro fator que demanda esforços de P,D&I em SIC e SegCiber no âmbito da APF diz respeito ao imposto pelo Decreto nº 8.135/2013, regulamentado pela Portaria Interministerial nº 141/2014, referente às soluções de comunicações de dados. Para tanto, a adequação dos órgãos e entidades da APF à legislação requer investimentos adequados e recorrentes em P,D&I.

A pesquisa, desenvolvimento e inovação nas áreas de SIC e SegCiber são pontos basilares para que o Estado brasileiro seja reconhecido mundialmente, como ator de destaque no cenário internacional, sendo respeitado por resultados tecnológicos relevantes, de forma a atender a necessidade de assegurar a soberania da Nação e, associado a isso, a privacidade de seus cidadãos no espaço cibernético.

Nesse sentido, são fundamentais a pesquisa e o desenvolvimento de soluções voltadas para a SIC e a SegCiber, baseadas em hardware e algoritmos criptográficos proprietários de Estado, com o objetivo de garantir a confidencialidade, integridade e autenticidade das comunicações estratégicas entre órgãos que integrem a APF, a exemplo da atuação da ABIN, por meio do Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC).

A exitosa iniciativa da Rede Nacional de Segurança da Informação e Criptografia – RENASIC não pode deixar de ser exemplificada. Criada em 2008 no GSI/PR e desde 2011 parte integrante do CDCiber/EB/MD, apresenta entre seus objetivos integrar pesquisadores de todo o país, fomentando o intercâmbio de conhecimentos e o desenvolvimento de novos projetos em segurança da informação e criptografia.

É essencial avançar na articulação para o fortalecimento e aceleração da implantação do ecossistema digital (SIC+SegCiber+Empresas+ICT) com a finalidade de apoiar o desenvolvimento de tecnologias de SIC e de SegCiber, a exemplo de soluções de reconhecimento de artefatos maliciosos e outras ferramentas cibernéticas, alavancando a criação do mesmo e promovendo maior sinergia com o ecossistema da defesa cibernética. Para tanto, faz-se necessário aprimorar os mecanismos de fomento e de financiamento que favoreçam parcerias entre o setor privado e as universidades e

institutos de pesquisa, para o desenvolvimento e a produção de soluções de SIC e de SegCiber.

Configura-se igualmente relevante a padronização do ambiente de SIC e de SegCiber no Governo Federal, por meio da criação de programas específicos que venham tanto a harmonizar especificações de bens e serviços, quanto a racionalizar e otimizar processos de compras governamentais.

Esse Objetivo Estratégico salienta o valor adicional de reforçar o quantitativo de empresas atuantes em SIC e SegCiber, na promoção de soluções e de tecnologias críticas para o Estado brasileiro, como Empresas Estratégicas de Defesa – EED, nos termos da Lei nº 12.598/2012, incentivando o desenvolvimento de soluções nacionais.

Para a implantação do arcabouço normativo de SIC e de SegCiber na APF, há que se buscar atualização permanente, seja de modelos de gestão, de soluções tecnológicas, de padrões, entre outros, acompanhando a dinâmica dos avanços das TIC e da convergência tecnológica.

OE-IV INSTITUIR MODELO DE GOVERNANÇA SISTÊMICA DE SIC E DE SEGCIBER NA APF, COM COORDENAÇÃO EXECUTIVA, ACOMPANHAMENTO E AVALIAÇÃO DO ÓRGÃO CENTRAL (GSI/PR)

O estabelecimento de um modelo de Governança Sistêmica de SIC e de SegCiber na APF, com a coordenação executiva, de acompanhamento e de avaliação do órgão central (GSI/PR), é essencial para a efetiva coordenação executiva das ações de Segurança da Informação e Comunicações e de Segurança Cibernética na APF, de modo a atender a transversalidade do tema, e contemplar ações multissetoriais que perpassem as competências dos órgãos da APF.

O GSI/PR terá entre seus desafios o de reforçar sua posição de coordenador executivo, bem como o de liderar as áreas de SIC e de SegCiber, em articulação e integração com os demais órgãos e entidades da APF, para consolidar seu papel de órgão central, promover a excelência de SIC e de SegCiber, em sinergia com as políticas públicas (Figura 2).

Para tanto, entre outras ações, estabelecerá um modelo de Governança Sistêmica de SIC e de SegCiber no âmbito da APF, de nível político estratégico (Anexo I), com a finalidade de: (i) apoiar a governança e a gestão; (ii) pactuar diretrizes; (iii) proporcionar harmonização nas iniciativas; (iv) incrementar o grau de maturidade; (v) aumentar a resiliência dos ativos de informação; (vi) fortalecer sistematicamente a segurança dos ativos de informação; e (vii) proteger as infraestruturas críticas de informação.

Os órgãos e entidades da APF, enquanto integrantes do sistema, no âmbito de suas competências, serão os agentes de formulação das orientações estratégicas em SIC e SegCiber, e atuarão de forma colaborativa para o fortalecimento e evolução do sistema como um todo e da excelência dessas áreas no âmbito do Governo Federal.

Este objetivo estratégico em particular contribui com os princípios norteadores desta Estratégia, em especial com os que se referem tanto ao estabelecimento de um sistema de âmbito nacional, quanto à formulação de uma “Política Nacional de Segurança da Informação e Comunicações e de Segurança Cibernética”.

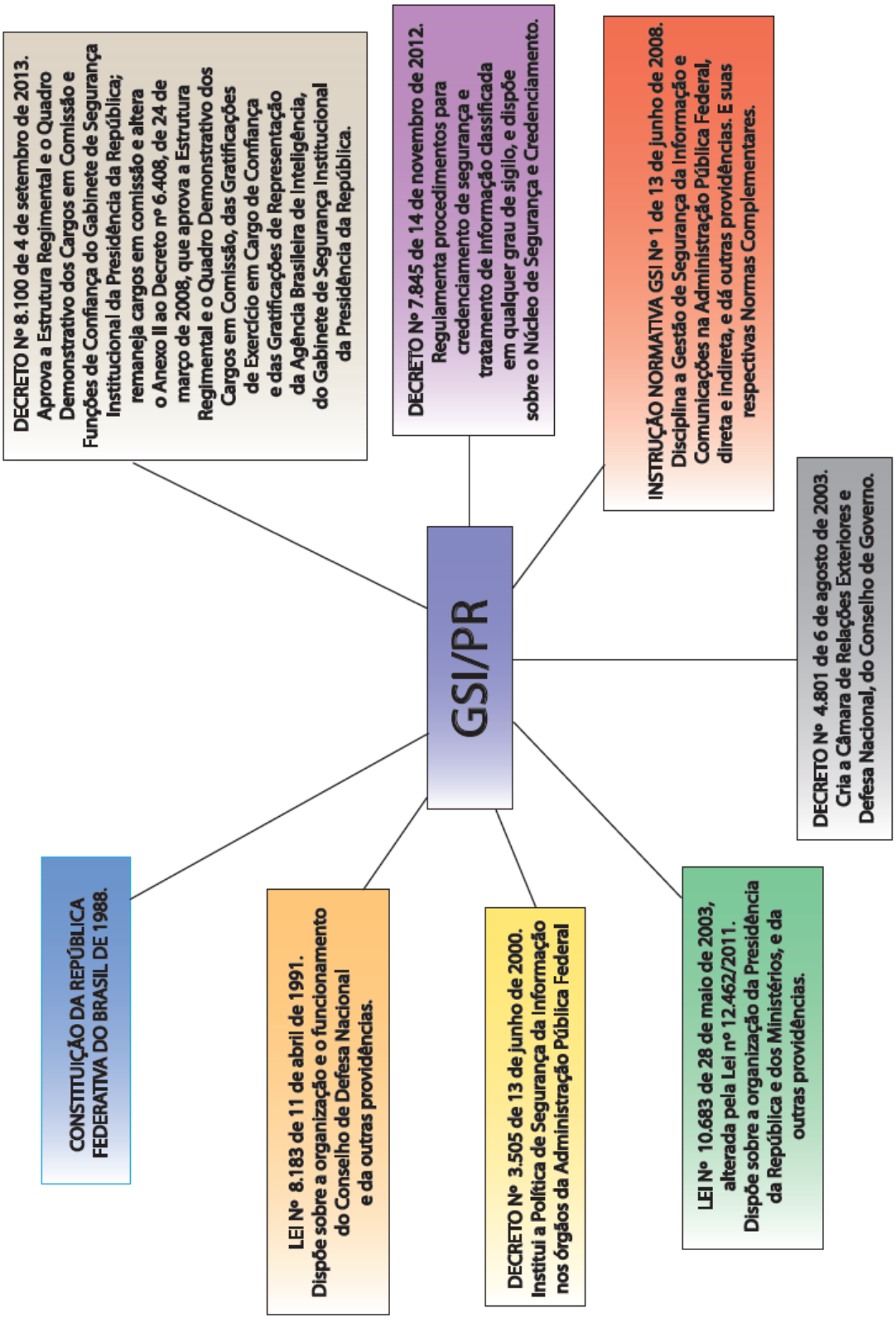


Figura 2 – Competências do GSI/PR em SIC e SegCiber

OE-V ALINHAR O PLANEJAMENTO DE SIC E DE SEGCIBER AO PLANEJAMENTO ESTRATÉGICO DOS ÓRGÃOS E ENTIDADES DA APF.

O planejamento estratégico institucional realizado no âmbito de cada órgão e entidade da APF encontra amparo no art. 6º do Decreto-Lei nº 200/1967 e deve guardar alinhamento com as diretrizes estratégicas do Governo e com o Plano Plurianual. Caracteriza-se como instrumento orientador, com abordagem de alto nível, que define, em linhas gerais, os rumos da organização e influencia as ações a serem empreendidas. Dessa forma, todo planejamento ou plano instituído no âmbito do órgão ou entidade deve guardar alinhamento com o planejamento estratégico institucional.

O planejamento das ações de SIC e de SegCiber é previsto na Norma Complementar nº 02/IN01/DSIC/GSI/PR – cuja observância é obrigatória e de responsabilidade da Alta Administração da APF, conforme concluiu o Acórdão 1.233/2012-TCU-Plenário em relação aos normativos publicados pelo GSI – e deve considerar os requisitos e pressupostos estabelecidos pelo planejamento estratégico institucional, bem como o disposto nesta Estratégia. O Acórdão 3.051/2014-TCU-Plenário, por sua vez, reforça tal necessidade de implementar o planejamento de SIC e de SegCiber na APF.

Nesta direção, cabe realçar aos órgãos e entidades da APF que, face ao nível estratégico das áreas de SIC e de SegCiber, a Política (POSIC), o Comitê Gestor de SIC e respectivas ações devem, também, estar alinhados ao nível estratégico institucional.

Portanto, é fundamental salientar não só a importância de um adequado planejamento de SIC e de SegCiber no âmbito dos órgãos e entidades da APF, mas o indispensável alinhamento entre este e o planejamento estratégico do órgão, visando que as ações de SIC e de SegCiber tenham o necessário apoio e patrocínio da Alta Administração, e estejam também alinhadas às diretrizes estratégicas do Governo, notadamente ao Plano Plurianual.

OE-VI AMPLIAR E FORTALECER AÇÕES COLABORATIVAS EM SIC E SEGCIBER COM A ACADEMIA, SETORES PÚBLICO, PRIVADO E TERCEIRO SETOR, NO PAÍS E NO EXTERIOR.

Os órgãos e entidades da APF devem buscar a articulação e o fortalecimento, nas áreas de SIC e de SegCiber, de ações colaborativas e de parcerias com o setor público, privado, academia e terceiro setor, no país e exterior para, dentre outras, a adoção de boas práticas, a busca de soluções tecnológicas e o estímulo ao desenvolvimento de produtos e serviços.

Tais ações devem ser entendidas como de elevada prioridade, no sentido de estimular o contínuo desenvolvimento de massa crítica, talentos e produtos nacionais, visando minimizar a dependência externa em benefício da sociedade e do Estado. Nessa direção, tal enfoque deve estar contemplado no planejamento de SIC e de SegCiber dos órgãos e entidades da APF, devidamente alinhado ao planejamento estratégico institucional.

A participação em fóruns e eventos nacionais e internacionais, como forma de ampliar a rede de conhecimento e as trocas de informação e experiências em SIC e SegCiber, contribui com o protagonismo do país nessas áreas. Neste sentido, a promoção e a disseminação de boas práticas de SIC e de SegCiber estimula um ciclo virtuoso de colaboração entre os atores.

Destaca-se ainda a importância da cooperação internacional bi e multilateral, no âmbito da SIC e da SegCiber, visando contribuir com o combate às ações ilícitas transnacionais.

Ações de colaboração e parcerias visam, dentre outras, a sinergia e a troca de experiências como forma de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, e aumentar a resiliência dos setores de SIC e de SegCiber no país, garantindo a disponibilidade e continuidade dos serviços públicos disponibilizados à sociedade, além de guardar estreita e especial relação com o “Objetivo Estratégico III - Garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF”.

OE-VII ELEVAR O NÍVEL DE MATURIDADE DE SIC E DE SEGCIBER NA APF.

A promoção de mudanças comportamentais na APF, alinhadas aos Programas Estratégicos de Governo e às legislações e normativos vigentes, são requisitos essenciais para a elevação do nível de maturidade em SIC e SegCiber.

Nesta direção, programas que promovam o acesso a informações e serviços públicos por meio eletrônico, a integração de sistemas e redes de informação pelos órgãos e entidades da APF e a modernização da gestão interna da administração pública, entre outros, impõem a incorporação de ações que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação, fortalecendo a maturidade de SIC e de SegCiber.

O arcabouço normativo de SIC e de SegCiber do GSI/PR apresenta temas que são complementares e interdependentes, e devem ser analisados e implantados nos órgãos e entidades da APF de forma holística, objetivando o estabelecimento de patamares de maturidade no curto, médio e longo prazo. Neste sentido, a promoção e a disseminação de boas práticas de SIC e de SegCiber estimula um ciclo virtuoso em busca da excelência.

Vale ressaltar que o cumprimento da legislação e dos normativos estabelecidos pelo GSI/PR é obrigatório e de responsabilidade da Alta Administração da APF, conforme concluiu o Acórdão 1.233/2012-TCU-Plenário, e sua não implementação, quando injustificada, é passível de sansões previstas em Lei.

Acrescenta-se que a Estratégia Geral de Tecnologia de Informação e Comunicações (EGTIC), coordenada pela SLTI/MP, no âmbito do SISP, caracteriza-se como um instrumento complementar para a melhoria contínua do nível de maturidade em SIC e SegCiber, ao promover que recursos adequados de tecnologia da informação e comunicação (TIC) sejam providos e implantados nos órgãos e entidades sob sua jurisdição.

Para visão global do nível de maturidade dos órgãos e entidades da APF, o GSI/PR, como coordenador e integrador desta Estratégia, inicialmente definirá os mecanismos de autodiagnóstico de SIC e de SegCiber, cujas informações servirão de base de conhecimento e permitirão maior clareza das vulnerabilidades da APF, visando tanto potencializar as ações orientadas à mitigá-las, quanto construir o indicador de nível de maturidade, promovendo a gestão, o acompanhamento e a avaliação, de forma continuada, colaborativa e sistêmica.

É imperativo, portanto, que os órgãos e entidades da APF estabeleçam os seus respectivos planejamentos nas áreas de SIC e de SegCiber, alinhados ao planejamento estratégico intitucional, contemplando ações para autodiagnóstico anual, bem como ações para o desenvolvimento de mecanismos internos de acompanhamento e avaliação sistemática do nível de maturidade, objetivando a excelência dessas áreas e, dentre outros resultados, a prevenção e o combate aos crimes cibernéticos no âmbito do Governo Federal.

OE-VIII REFORÇAR A SIC E A SEGCIBER COMO ALTA PRIORIDADE NA AGENDA DE GOVERNO.

Os impactos causados por falhas na SIC e na SegCiber, no âmbito dos órgãos e entidades da APF, prejudicam a imagem do governo e afetam a adequada prestação de serviços públicos à sociedade. Desta forma, considerar a SIC e a SegCiber como temas prioritários no âmbito das políticas públicas é fator essencial na manutenção da credibilidade do Estado.

No cenário mundial, verifica-se que as áreas de SIC e de SegCiber são tratadas no mais alto grau estratégico, a exemplo das estratégias nacionais de segurança cibernética publicadas. De modo semelhante, diversos eventos têm sido promovidos para tratar do assunto, inclusive com a presença de líderes de Estado. Tais fatos demonstram cada vez mais a preocupação dos países com a SIC e a SegCiber.

No Brasil, as áreas de SIC e de SegCiber estão caracterizadas no Governo Federal, dentre outros, conforme a seguir: (i) o art. 91 da Constituição Federal institui o Conselho de Defesa Nacional (CDN), órgão de consulta do Presidente da República acerca de assuntos relacionados à soberania nacional e à defesa do Estado democrático; (ii) a Câmara de Relações Exteriores e Defesa Nacional (CREDEN) do Conselho de Governo tem como finalidade tratar de matérias como a cooperação internacional em assuntos de segurança e defesa, segurança para infraestruturas críticas, segurança da informação e segurança cibernética; (iii) documento oficial anual denominado “Mensagem Presidencial”, encaminhado pelo Presidente da República ao Poder Legislativo quando da abertura dos trabalhos da legislatura, o tema segurança da informação tem seu destaque no subitem soberania nacional; e (iv) o art. 6º da Lei nº 10.683/2003 estabelece ao GSI/PR, entre outras atribuições, a coordenação da segurança da informação.

No entanto, ainda que tais áreas se mostrem cada dia mais relevantes e cruciais, ainda não são tratadas como alta prioridade na agenda de governo, com apoio efetivo da Alta Administração. Urge, então, aumentar gradativa e prioritariamente o nível de maturidade e estabeler a Governança Sistêmica de SIC e de SegCiber na APF, ponto de partida para uma política e um sistema nacional abrangendo todos os entes federativos e o três poderes, o que caracterizará a alta prioridade na agenda do governo, contribuindo com o êxito de programas tais como “Bem Mais Simples Brasil” e “Governo Digital”.

OE-IX VALORIZAR E AMPLIAR AÇÕES QUE FORTALEÇAM A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO.

O GSI/PR define como infraestruturas críticas as instalações, os serviços, os bens e os sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade. No tocante às infraestruturas críticas nacionais, tais como energia, telecomunicações, transportes, água, finanças, informação, dentre outras, é cada vez mais elevada a interdependência, o que impacta as redes e sistemas de informação para a sua gerência e controle.

Por sua vez, a segurança das infraestruturas críticas da informação refere-se à proteção do subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. Os ativos de informação são os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Para a consecução deste objetivo estratégico, é fundamental, portanto, que cada instituição planeje e invista os recursos necessários ao fortalecimento da segurança de seus ativos de informação, sem que se perca o foco no fortalecimento das ações cooperativas entre as instituições do setor público e dessas com a academia e o setor privado.

Conforme constante no "Guia de Referência para a Segurança das Infraestruturas Críticas da Informação" publicado pelo GSI/PR, as instituições responsáveis pelas infraestruturas críticas nacionais são orientadas a realizar, no mínimo: (i) mapeamento de seus ativos de informação para a identificação daqueles que são críticos; (ii) gestão de risco, com identificação de potenciais ameaças e vulnerabilidades; e (iii) estabelecimento de método de geração de alerta de segurança das infraestruturas críticas da informação.

Ressalta-se, por fim, o quão fundamental para o Estado é o envolvimento de todas as instâncias para o incremento do nível de segurança das infraestruturas críticas, destacando-se a necessidade de fortalecimento da interação entre os órgãos e entidades da APF e setores envolvidos no funcionamento das infraestruturas críticas nacionais, e de respectiva normatização.

OE-X PROMOVER MECANISMOS DE CONSCIENTIZAÇÃO DA SOCIEDADE SOBRE SIC E SEGCIBER.

A conscientização sobre SIC e SegCiber deve ser tratada como instrumento de mudança cultural, envolvendo cada vez mais a integração dos órgãos e entidades da APF e a sociedade brasileira, com o objetivo de levar a um processo continuado de postura responsável e consciente dos aspectos relacionados a SIC e a SegCiber.

No cenário mundial, várias ações de conscientização têm sido promovidas por meio de campanhas periódicas, de alcance nacional, a exemplo de países como Estados Unidos da América, Japão e Canadá, bem como na Comunidade Européia.

No Brasil, podemos citar o “Dia da Segurança da Informação”, promovido pelo TCU; a Cartilha de Segurança para Internet, publicada pelo Comitê Gestor da Internet no Brasil (CGI.br); e o “Dia Internacional de Segurança em Informática (DISI)”, promovido pela Rede Nacional de Ensino e Pesquisa (RNP), entre outras iniciativas.

No tocante às áreas de SIC e de SegCiber, para o uso seguro e responsável das tecnologias de informação e comunicação, é importante que se promovam ações periódicas junto à sociedade, que visem a garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, alcançando, dentre outros resultados, a prevenção de crimes cibernéticos e a proteção da privacidade.

METAS DA ESTRATÉGIA

Tendo em vista a natureza transversal dos Objetivos Estratégicos de SIC e de SegCiber apresentados anteriormente, as metas foram construídas a partir de uma visão holística, ou seja, considerando a Estratégia como um todo, não se vinculando necessariamente cada meta a um único objetivo estratégico.

Assim sendo, as metas são apresentadas a seguir de forma distribuída em espaços temporais, no quadriênio 2015-2018.

Em 2015

M-I: Definir metodologia e mecanismo de autodiagnóstico de SIC e de SegCiber da APF.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI.

M-II: Atingir no mínimo **25%** da **APF direta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-III: Articular e estabelecer programa no PPA 2016-2019 que contemple conjuntamente as temáticas de SIC e de SegCiber.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos órgãos competentes.

M-IV: Articular e formalizar função orçamentária específica em Segurança Institucional, contemplando subfunção SIC e SegCiber, entre outras.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos órgãos competentes.

M-V: Criar a Câmara Multissetorial de SIC e de SegCiber da APF no âmbito do Sistema.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

M-VI: Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com a ENAP/MP para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.

Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-VII: Propor um guia de boas práticas de planejamento de SIC e de SegCiber para os órgãos e entidades da APF, com base na Norma Complementar nº 02/IN01/DSIC/GSIPR, visando seu alinhamento ao planejamento estratégico institucional.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

M-VIII: Propor a criação do "Dia Oficial de SIC e de SegCiber do Governo Federal"
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

Em 2016

M-IX: Estabelecer o Modelo de Governança Sistêmica de SIC e de SegCiber da APF – nível político estratégico.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

M-X: Estabelecer mecanismo para mapeamento sistemático dos ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade que compõem as infraestruturas críticas da informação.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

M-XI: Atingir no mínimo **50%** da **APF direta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XII: Atingir no mínimo **5%** da **APF indireta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XIII: Desenvolver indicador de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF, como um mecanismo de acompanhamento e avaliação. O desenvolvimento envolverá, dentre outras, as etapas de debate metodológico, estudos e testes e a definição do indicador.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI.

M-XIV: Articular a inserção das áreas de SIC e de SegCiber no Programa Nacional de Gestão Pública e Desburocratização (GesPública), coordenado pelo MP, no item "Informação e Conhecimento".
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração do órgão competente.

M-XV: Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e SegCiber, visando a formação continuada dos agentes públicos nestas áreas.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-XVI: Articular a criação do ecossistema digital (SIC+SegCiber+Empresas+ICTs), em sintonia com o ecossistema de defesa cibernética.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração do órgão competente.

M-XVII: Criar a Comissão para estudo de viabilidade da criação de carreira de Estado de SIC e de SegCiber e respectiva estrutura organizacional, em nível estratégico, no Governo Federal.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos órgãos competentes e demais atores do sistema de SIC e de SegCiber da APF.

M-XVIII: Criar Grupo de Trabalho objetivando a modelagem e o planejamento de exercícios de ataques cibernéticos às redes da APF.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos órgãos competentes e demais atores do sistema de SIC e de SegCiber da APF.

M-XIX: Promover a "Conferência Bianual de SIC e de SegCiber da APF".
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

Em 2017

M-XX: Implementar e aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF, como mecanismo de acompanhamento e avaliação.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI.

M-XXI: Atingir no mínimo **75%** da **APF direta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XXII: Atingir no mínimo **10%** da **APF indireta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XXIII: Propor método de identificação de ameaças e geração de alertas das infraestruturas críticas da informação.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI e da Câmara Multissetorial de SIC e de SegCiber da APF e demais atores do sistema de SIC e de SegCiber da APF.

M-XXIV: Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-XXV: Encaminhar o resultado do Grupo de Trabalho de modelagem e planejamento de exercícios de ataques cibernéticos às redes da APF ao órgão central (GSI/PR).
Responsáveis: Grupo de Trabalho criado na M-XVIII.

Em 2018

M-XXVI: Aferir o indicador anual de nível de maturidade de SIC e de SegCiber nos órgãos e entidades da APF.
Responsável: órgão central (GSI/PR).

M-XXVII: Atingir **100%** da **APF direta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XXVIII: Atingir no mínimo **15%** da **APF indireta** com autodiagnóstico de SIC e de SegCiber acompanhados e avaliados pelo órgão central (GSI/PR).
Responsável: órgão central (GSI/PR), com assessoramento do CGSI.

M-XXIX: Formalizar parceria do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com, no mínimo, mais duas Escolas de Governo, para inserção de cursos e/ou de disciplinas de SIC e de SegCiber, visando a formação continuada dos agentes públicos nestas áreas.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-XXX: Levantar novos elementos estratégicos e elaborar a "Estratégia de SIC e de SegCiber da APF 2019-2022".
Responsável: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos atores do sistema de SIC e de SegCiber da APF.

M-XXXI: Encaminhar o resultado do estudo de viabilidade de criação da carreira de Estado de SIC e de SegCiber no Governo Federal ao órgão central (GSI/PR).
Responsáveis: Comissão criada na M-XVII.

M-XXXII: Promover a "Conferência Bianual de SIC e de SegCiber da APF".
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos demais atores do sistema de SIC e de SegCiber da APF.

Metas contínuas: 2015 a 2018

M-XXXIII: Promover anualmente, no âmbito da APF, no mínimo 10 oficinas abordando as Normas Complementares à IN GSI/PR nº 01/2008.
Responsáveis: órgãos e entidades da APF.

M-XXXIV: Anualmente, promover e coordenar no mínimo 2 Colóquios Técnicos sobre tratamento e respostas a incidentes em redes computacionais da APF.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-XXXV: Alinhar, de forma contínua, o planejamento de SIC e de SegCiber dos órgãos e entidades da APF aos respectivos Planejamentos Estratégicos.
Responsáveis: órgãos e entidades da APF.

M-XXXVI: Fortalecer e formalizar parcerias do órgão central do sistema de SIC e de SegCiber da APF (GSI/PR) com universidades e instituições de ensino superior para inserção de cursos e/ou de disciplinas de SIC e de SegCiber no nível da graduação e da pós graduação.
Responsáveis: órgão central (GSI/PR), com o assessoramento do CGSI.

M-XXXVII: Avaliar e revisar a “Estratégia de SIC e de SegCiber da APF 2015-2018”.
Responsáveis: órgão central (GSI/PR), com assessoramento do CGSI e colaboração dos atores do sistema de SIC e de SegCiber da APF.

M-XXXVIII: Promover campanhas de conscientização da sociedade nas áreas de SIC e de SegCiber.
Responsáveis: atores do sistema de SIC e de SegCiber da APF.

DISPOSIÇÕES FINAIS

Esta Estratégia aplica-se a todos os órgãos e entidades da APF, entrará em vigor na data de sua publicação no Diário Oficial da União e terá validade no quadriênio 2015-2018, sendo revisada, periodicamente, em consonância com as contribuições das instâncias de assessoramento e apoio à decisão do Modelo de Governança Sistêmica de SIC e de SegCiber da APF, buscando atender as demandas dos órgãos e entidades que integram o Sistema, em prol do alcance da visão de futuro desta Estratégia.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 38500**: Governança Corporativa de Tecnologia da Informação. Rio de Janeiro, 2006.

AUSTRALIAN GOVERNMENT. **Australian Government Information Security Manual – Principles - Australian**, 2014. Disponível em: <http://www.asd.gov.au/publications/Information_Security_Manual_2014_Principles.pdf>. Acesso em Fevereiro de 2015.

AUSTRALIAN GOVERNMENT. **Cyber Security Strategy 2011**, Austrália, 2011. Disponível em: <http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>. Acesso em Fevereiro de 2015.

BLUE COAT SYSTEMS. **The Inception Framework:** Cloud-Hosted APT by Snorre Fagerland and Waylon Grange Blue Coat Systems, Inc., 2014. Disponível em: < https://www.bluecoat.com/documents/download/638d602b-70f4-4644-aaad-b80e1426aad4/d5c87163-e068-440f-b89e-e40b2f8d2088>. Acesso em Fevereiro de 2015.

BRASIL. Congresso. Senado Federal. Comissão Parlamentar de Inquérito. **CPI da Espionagem - Relatório Final**. Brasília, DF, 2014.

BRASIL. Conselho Nacional de Justiça. **Resolução Nº 99, de 24 de novembro de 2009**. Anexo I: A Estratégia de TIC do Poder Judiciário, Brasília, DF, 2009. Disponível em: <http://www.cnj.jus.br/images/stories/docs_cnj/resolucao/anexorescnj_99.pdf>. Acesso em Fevereiro de 2015.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília, DF: Senado, 1988.

BRASIL. **Decreto nº 3.505 de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2000.

BRASIL. **Decreto nº 3.996 de 31 de outubro de 2001**. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2001.

BRASIL. **Decreto nº 4.801, de 6 de agosto de 2003**. Cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Casa Civil, Subchefia para Assuntos Jurídicos, 2003.

BRASIL. **Decreto nº 4.829, de 3 de setembro de 2003**. Dispõe sobre a criação do Comitê Gestor da Internet no Brasil - CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2003.

BRASIL. **Decreto nº 5.563, de 11 de outubro de 2005.** Regulamenta a Lei nº 10.973, de 2 de dezembro de 2004, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2005.

BRASIL. **Decreto nº 6.605, de 14 de outubro de 2008**. Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC. Casa Civil, Subchefia para Assuntos Jurídicos, 2008.

BRASIL. **Decreto nº 6.703 de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2008.

BRASIL. **Decreto nº 7.009, de 12 de novembro de 2009**. Dá nova redação aos arts. 1º, 2º e 3º do Decreto no 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Casa Civil, Subchefia para Assuntos Jurídicos, 2009.

BRASIL. **Decreto nº 7.579, de 11 de outubro de 2011**. Dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal. Casa Civil, Subchefia para Assuntos Jurídicos, 2011.

BRASIL. **Decreto nº 7.724 de 16 de maio de 2012**. Regulamenta a Lei no 12.527, de 18 de novembro de 2011. Casa Civil, Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Decreto nº 7.845 de 14 de novembro de 2012**. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Casa Civil, Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Decreto nº 8.096, de 4 de setembro de 2013**. Altera o Decreto nº 4.801, de 6 de agosto de 2003, que cria a Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo. Casa Civil, Subchefia para Assuntos Jurídicos, 2013.

BRASIL. **Decreto nº 8.135 de 4 de novembro de 2013**. Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. Casa Civil, Subchefia para Assuntos Jurídicos, 2013.

BRASIL. **Decreto nº 8.414, de 26 de fevereiro de 2015**. Institui o Programa Bem Mais Simples Brasil e cria o Conselho Deliberativo e o Comitê Gestor do Programa. Casa Civil, Subchefia para Assuntos Jurídicos, 2015.

BRASIL. **Decreto-lei nº 200, de 25 de fevereiro de 1967**. Dispõe sôbre a organização da Administração Federal, estabelece diretrizes para a Reforma Administrativa e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2015.

BRASIL. **Lei nº 6.880, de 30 de dezembro de 1980**. Dispõe sobre o Estatuto dos Militares. Casa Civil, Subchefia para Assuntos Jurídicos, 1980.

BRASIL. **Lei nº 10.683, de 28 de maio de 2003**. Dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2003.

BRASIL. **Lei nº 10.973, de 2 de dezembro de 2004**. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2004.

BRASIL. **Lei nº 11.079, de 30 de dezembro de 2004.** Institui normas gerais para licitação e contratação de parceria público privada no âmbito da administração pública. Casa Civil, Subchefia para Assuntos Jurídicos, 2004.

BRASIL. **Lei nº 12.527 de 18 de novembro de 2011.** Regula o acesso a informações. Casa Civil, Subchefia para Assuntos Jurídicos, 2011.

BRASIL. **Lei nº 12.593 de 18 de janeiro de 2012**. Institui o Plano Plurianual da União para o período de 2012 a 2015. Casa Civil, Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Lei nº 12.598, de 21 de março de 2012**. Estabelece normas especiais para as compras, as contratações e o desenvolvimento de produtos e de sistemas de defesa; dispõe sobre regras de incentivo à área estratégica de defesa; altera a Lei nº 12.249, de 11 de junho de 2010; e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2012.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Casa Civil, Subchefia para Assuntos Jurídicos, 2014.

BRASIL. **Lei nº 8.183 de 11 de abril de 1991**. Dispõe sobre a organização e o funcionamento do Conselho de Defesa Nacional e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 1991.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Casa Civil, Subchefia para Assuntos Jurídicos, 2001.

BRASIL. Ministério da Defesa. Exército Brasileiro. **Diretriz Ministerial nº 14/2009, de 9 de novembro de 2009**. Atribuiu ao Exército Brasileiro a responsabilidade pela coordenação e integração do Setor Cibernético do Ministério da Defesa. Brasília, DF, MD/EB, 2009.

BRASIL. Ministério da Defesa. **Portaria Normativa nº 2.777/MD, de 27 de outubro de 2014**. Dispõe sobre a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 28 out. 2014. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=7&data=28/10/2014>. Acesso em Março de 2015.

BRASIL. Ministério da Defesa. **Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012**. Dispõe sobre a Política Cibernética de Defesa. Diário Oficial da República Federativa do Brasil, Brasília, DF, 27 dez. 2014. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=11&data=27/12/2012>. Acesso em Março de 2015.

BRASIL. Ministério do Planejamento, Orçamento e Gestão, Sistema de Administração de Recursos de Tecnologia da Informação. **Estratégia Geral de Tecnologia da Informação e Comunicações – EGTIC 2014-2015**, Brasília, DF, MP/SLTI, 2014.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Instituto Brasileiro de Geografia e Estatística. **Pesquisa Nacional por Amostra de Domicílios – PNAD 2012**. Rio de Janeiro, MP/IBGE, v.32, 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Portaria Interministerial nº 141, de 2 de maio de 2014**. Diário Oficial da República Federativa do Brasil, Brasília, DF, 5 mai. 2014. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=82&data=05/05/2014>. Acesso em Março de 2015.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Gestão. **Melhoria da gestão pública por meio da definição de um guia referencial para medição do desempenho da gestão, e controle para o gerenciamento dos indicadores de eficiência, eficácia e de resultados do programa nacional de gestão pública e desburocratização** - Produto 4: Guia Referencial para Medição de Desempenho e Manual para Construção de Indicadores. Brasília, DF, MP/SEGES, 2009.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. **Planejamento estratégico 2011-2014**. Brasília, DF, MP/SLTI, 2010.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação. **Planejamento estratégico 2011-2015**. 4ª ed., 5ª Versão – Brasília, DF, MP/SLTI, 2014.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Secretaria de Planejamento e Investimentos Estratégicos. **Plano Mais Brasil – PPA 2012 – 2015**. Brasília, DF, MP/SPI, 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Sistema de Administração de Recursos de Tecnologia da Informação. **Estratégia Geral de Tecnologia da Informação do SISP 2013-2015**: versão 1.0. Brasília, DF, MP/SLTI, 2012.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. Sistema de Administração de Recursos de Informática e Informação. **Estratégia Geral de Tecnologia da Informação 2008**. Brasília, DF, MP/SLTI, 2008.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde : segurança cibernética no Brasil**, organização Claudia Canongia e Raphael Mandarino Junior. Brasília, DF, GSIPR/SE/DSIC, 2010.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008**. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, DF, GSI/PR, 2008.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 01/IN01/DSIC/GSI/PR**. Atividade de Normatização. Brasília, DF, GSI/PR, 2008.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 02/IN01/DSIC/GSI/PR**. Metodologia de Gestão de Segurança da Informação e Comunicações. Brasília, DF, GSI/PR, 2008.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 03/IN01/DSIC/GSI/PR**. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2009.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 04/IN01/DSIC/GSI/PR – Rev1**. Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 05/IN01/DSIC/GSI/PR**. Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2009.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 06/IN01/DSIC/GSI/PR**. Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Brasília, DF, GSI/PR, 2009.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 07/IN01/DSIC/GSI/PR – Rev1**. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 08/IN01/DSIC/GSI/PR**. Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Brasília, DF, GSI/PR, 2010.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 09/IN01/DSIC/GSI/PR – Rev2**. Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 10/IN01/DSIC/GSI/PR**. Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 11/IN01/DSIC/GSI/PR**. Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 12/IN01/DSIC/GSI/PR**. Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 13/IN01/DSIC/GSI/PR**. Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 14/IN01/DSIC/GSI/PR**. Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 15/IN01/DSIC/GSI/PR**. Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 16/IN01/DSIC/GSI/PR**. Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. Brasília, DF, GSI/PR, 2012.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 17/IN01/DSIC/GSI/PR**. Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 18/IN01/DSIC/GSI/PR**. Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 19/IN01/DSIC/GSI/PR**. Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas

Estruturantes da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 20/IN01/DSIC/GSI/PR – Rev1**. Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Brasília, DF, GSI/PR, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Instrução Normativa GSI/PR nº 01, de 13 de junho de 2008. **Norma Complementar nº 21/IN01/DSIC/GSI/PR**. Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta. Brasília, DF, GSI/PR, 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa GSI/PR nº 02, de de 5 de fevereiro de 2013**. Dispõe sobre o Credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal. Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Instrução Normativa GSI/PR nº 03, de de 6 de março de 2013**. Dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal. Brasília, DF, GSI/PR, 2013.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 31 – GSIPR/CH, de 06 de outubro de 2008**. Institui a Rede Nacional de Segurança da Informação e Criptografia - RENASIC. Brasília, DF, GSI/PR, 2008.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Portaria nº 45, de 8 de setembro de 2009**. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Diário Oficial [da] República Federativa do Brasil, Brasília, DF, 9 set. 2009. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=09/09/2009>. Acesso em Março de 2015.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Guia de referência para a segurança das infraestruturas críticas da informação**; organização Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior. Brasília, DF, PR/GSI/SE/DSIC, 2010.

BRASIL. Presidência da República. Portal Brasil. PNAD 2012: Percentual de internautas cresce nas regiões Norte e Nordeste. 2013. Disponível em: < http://www.brasil.gov.br/infraestrutura/2013/09/percentual-de-internautas-cresce-nas-regioes-norte-e-nordeste-em-2012/>. Acesso em: Março de 2015.

BRASIL. Presidência da República. Secretaria de Assuntos Estratégicos. **Brasil 2022** / Secretaria de Assuntos Estratégicos. Brasília: Presidência da República, Secretaria de Assuntos Estratégicos - SAE, 2010. 100 p.

BRASIL. TCU. **Acórdão 1.145/2011-TCU-Plenário**. 2011. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20110512/AC_1145_15_11_P.doc>. Acessado em: Março de 2015.

BRASIL. TCU. **Acórdão 1.233/2012-TCU-Plenário**. 2012. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20120528/AC_1233_19_12_P.doc>. Acessado em: Março de 2015.

BRASIL. TCU. **Acórdão 2.308/2010-TCU-Plenário**. 2010. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20100913/AC_2308_33_10_P.doc>. Acessado em: Março de 2015.

BRASIL. TCU. **Acórdão 2.585/2012-TCU-Plenário**. 2012. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20121112/AC_2585_38_12_P.doc>. Acessado em: Março de 2015.

BRASIL. TCU. **Acórdão 3.051/2014-TCU-Plenário**. 2014. Disponível em: <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141107/AC_3051_44_14_P.doc>. Acessado em: Março de 2015.

BRASIL. TCU. **Acórdão 3.117/2014-TCU-Plenário**. 2014. Disponível em: < <http://www.tcu.gov.br/Consultas/Juris/Docs/judoc/Acord/20141114/AC_3117_45_14_P.doc>. Acessado em: Março de 2015.

COMISÃO EUROPEIA. **Comunicação da comissão ao parlamento europeu, ao conselho, ao comité económico e social europeu e ao comité das regiões.** Uma Agenda Digital para a Europa, 2010. Disponível em: <http://www.umic.pt/images/stories/publicacoes3/Digital%20Agenda%20Comunic%20COM%202010-05-19%20PT.pdf>. Acesso em Fevereiro de 2015.

E-BIT. **Evolução da Internet e do e-commerce**. Faturamento anual do e-commerce no Brasil – Bilhões. Disponível em: < http://www.e-commerce.org.br/stats.php>. Acesso em: Março de 2015.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA), **National Cyber Security Strategies - Practical Guide on Development and Execution**, European Network and Information Security Agency (ENISA), dezembro de 2012. Disponível em: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide/at_download/fullReport>. Acesso em Fevereiro de 2015.

EUROPEAN NETWORK AND INFORMATION SECURITY AGENCY (ENISA). **National Cyber Security Strategies - Setting the course for national efforts to strengthen security in cyberspace**, maio de 2012. Disponível em: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper/at_download/fullReport >. Acesso em Fevereiro de 2015.

EUROPEAN UNION. **Cyber security Strategy of the European Union**. An Open, Safe and Secure Cyberspace European Commission, JOIN Final, 2013. Disponível em: <http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf>. Acesso em Fevereiro de 2015.

GERMANY - FEDERAL MINISTRY OF THE INTERIOR. **Cyber Security Strategy for Germany**, 2011**.** Disponível em: <https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CyberSecurity/Cyber_Security_Strategy_for_Germany.pdf?__blob=publicationFile>. Acesso em Fevereiro de 2015.

GOVERNMENT OF CANADA. **Canada's Cyber Security Strategy. For a stronger and more prosperous Canada**, 2010. Disponível em: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf>. Acesso em Fevereiro de 2015.

IT GOVERNANCE INSTITUTE. **COBIT 5: Modelo Corporativo para Governança e Gestão de TI**. ISACA. 2012.

ITALY - PRESIDENCY OF THE COUNCIL OF MINISTERS. **National Strategic Framework for Cyberspace Security**, 2014. Disponível em: <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf>. Acesso em Fevereiro de 2015.

KAPLAN, R. S.; NORTON, D. P.; **Using the Balanced Scorecard as a Strategic Management System**, Harvard Business Review, p. 75-85, Jan/Fev, 1996.

KENYA - MINISTRY OF INFORMATION. **Communications and Technology. National Cybersecurity Strategy 2014**, 2014. Disponível em: <http://www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf>. Acesso em Fevereiro de 2015.

LUIIJF, E.; BESSELING, K.; DE GRAAF, P.; **Nineteen National Cyber Security Strategies**, Int. J. Critical Infrastructures, Vol. 9, Nºs. 1/2, 2013. Disponível em: < http://www.researchgate.net/profile/Eric_Luiijf/publication/261950643_Nineteen_National_Cyber_Security_Strategies/links/543545380cf2bf1f1f286509.pdf>. Acesso em Fevereiro de 2015.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Cyber security Framework Development Overview**. NIST's Role in Implementing Executive Order

13636, Improving Critical Infrastructure Cybersecurity, Presentation to ISPAB, 2013. Disponível em: <http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_sedgewick.pdf>. Acesso em Fevereiro de 2015.

NEW ZEALAND GOVERNMENT. **New Zealand's Cyber Security Strategy**, 2011. Disponível em: <http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf>. Acesso em Fevereiro de 2015.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). **Cybersecurity Policy Making at a Turning Point**: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy, OECD Digital Economy Papers, No. 211, OECD Publishing, 2012. Disponível em: <http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf>. Acesso em Fevereiro de 2015.

SILVA, Leandro Costa da. **O Balanced Scorecard e o Processo Estratégico**. Caderno de Pesquisas em Administração. São Paulo, v. 10, nº 4, p. 61-73, outubro/dezembro de 2003.

SILVA, Roselito Felix da. **Proposta de Adaptação do Modelo Balanced Sorecard – BSC para a Gestão de Segurança da Informação em Órgãos Da Administração Pública**, Dissertação de Mestrado em Engenharia Elétrica, UnB, Brasília, DF, 2010.

SILVA, Roselito Felix da; FELIX, Patrícia do Prado; TIMÓTEO, Rafael; **Balanced Scorecard: Adequação Para a Gestão Estratégica nas Organizações Públicas**; Revista do Serviço Público Brasília 62 (1): p. 51-74, Jan/Mar 2011.

SWITZERLAND. **National strategy for the protection of Switzerland against cyber risks**, 2012. Disponível em: <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/National_strategy_for_the_protection_of_Switzerland_against_cyber_risksEN.pdf>. Acesso em Fevereiro de 2015.

TAKAHASHI, Tadao (org.). **Livro verde da Sociedade da Informação no Brasil**. Brasília, DF, Ministério da Ciência e Tecnologia, 2000.

UNITED KINGDOM. **The UK Cyber Security Strategy**. Protecting and promoting the UK in a digital world, 2011. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf>. Acesso em Fevereiro de 2015.

UNITED NATIONS. General Assembly. **Resolution 68/167.** The right to privacy in the digital age. United Nations Publications , United States, 2013. Disponível em: <http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167>. Acesso em: Março de 2015.

UNITED STATES. Government Accountability Office. **National Strategy, Roles, and Responsibilities Need to Be Better Defined and More Effectively,** 2013. Disponível em: <http://www.gao.gov/assets/660/652170.pdf>. Acesso em fevereiro de 2015.

UNITED STATES. Seal of the President Of the United States. **International Estrategy for Cyberspace**, Prosperity, Security, and Openness in a Networked World, 2011. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em Fevereiro de 2015.

UNITED STATES. Seal of the President of the United States. **National Security Strategy,** 2015. Disponível em: <http://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf>. Acesso em Fevereiro de 2015.

UNITED STATES. **USA - Cyber Space Policy Review - Assuring a Trusted and Resilient Information and Communications Infrastructure**, Review Final, 2009. Disponível em: <https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em Fevereiro de 2015.

WAMALA, Frederick. **The ITU National Cybersecurity Strategy Guide**, International Telecommunications Union (ITU), 2011. Disponível em: <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>. Acesso em Fevereiro de 2015.

WORLD CONFERENCE ON INTERNATIONAL TELECOMMUNICATIONS, WCIT-12, 2012, Dubai. **Final Acts of the World Conference on International Telecommunications (WCIT-12).** Switzerland, International Telecommunication Union (ITU), 2012.

WORLD ECONOMIC FORUM – **Report of WEF/2014**. 2014. Disponível em: <http://www.weforum.org/reports/global-risks-2014-report

WORLD ECONOMIC FORUM – **Report of WEF/2015**, 2015. Disponível em: <http://reports.weforum.org/global-risks-2015/

ZIMMERMAN, Carson. **Ten Strategies of a World-Class Cybersecurity Operations Center**, The MITRE Corporation, 2014. Disponível em: <http://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf>. Acesso em Fevereiro de 2015.

ANEXO I

MODELO DE GOVERNANÇA SISTÊMICA DE SIC E DE SEGCIBER DA APF - NÍVEL POLÍTICO ESTRATÉGICO

De acordo com o Decreto-Lei nº 200, de 25 de fevereiro de 1967, as atividades administrativas no âmbito da administração pública federal direta, autárquica e fundacional estão organizadas sob a forma de sistemas, com a finalidade de uniformizar a interpretação e aplicação da legislação, bem como de padronizar os procedimentos a serem realizados, visando a sua eficiência.

Dessa forma, o Modelo de Governança Sistêmica de SIC e de SegCiber da APF (Figura 3), de nível político estratégico, apoiará o estabelecimento de competências e respectivas responsabilidades entre os órgãos e entidades da APF de forma a: (i) somar e otimizar esforços; (ii) pactuar ações em prol dos avanços das áreas e efetividade nos resultados; (iii) buscar a excelência da gestão e da maturidade; (iv) estabelecer mecanismos e critérios de acompanhamento e avaliação contínuos; e (v) promover a articulação multissetorial e a inovação.

Integram o Modelo de Governança Sistêmica de SIC e de SegCiber da APF:

a) **Órgão Central (GSI/PR)** : órgão gestor superior das áreas de SIC e de SegCiber, exercerá a coordenação executiva e a integração das ações na definição das respectivas diretrizes político estratégicas daquelas áreas no âmbito da APF.
b) **Órgãos Gestores Setoriais Nível A**: são representados pelos Ministérios e equivalentes, no âmbito da APF, participantes da cadeia de valor e dos pactos para implantação das diretrizes estratégicas.
c) **Órgãos Gestores Setoriais Nível B**: são representados pelos órgãos e entidades vinculados diretamente aos Órgãos Gestores Setoriais Nível A, no âmbito da APF, participantes da cadeia de valor e dos pactos alavancados pelos respectivos Órgãos Gestores Setoriais Nível A, para implantação das diretrizes estratégicas.
d) **Órgãos Gestores Seccionais:** são representados pelos órgãos e entidades vinculados diretamente aos Órgãos Gestores Setoriais Nível B, no âmbito da APF, participantes da cadeia de valor e dos pactos alavancados pelos respectivos Órgãos Gestores Setoriais Nível B, para implantação das diretrizes estratégicas.

e) **Órgãos e Instituições Colaboradoras**: são representados por instituições de governo (demais entes federativos), da academia, do setor privado e do terceiro setor, que mantenham vínculo de qualquer natureza com os órgãos e entidades da APF, sejam Órgãos Gestores Setoriais Nível A, Órgãos Gestores Setoriais Nível B ou Órgãos Gestores Seccionais.

f) **Instâncias de assessoramento e apoio à decisão do Sistema de SIC e SegCiber da APF**:

I. **Comitê Gestor de Segurança da Informação** (CGSI/CDN): comitê de nível estratégico que assessora a Secretaria Executiva do CDN nas questões relativas à segurança da informação, o qual se reúne mensalmente sob a coordenação do GSI/PR, e conta com 17 órgãos da APF, será consultado, no âmbito deste Sistema, como apoio nas deliberações das diretrizes e normativos de SIC e SegCiber da APF. O CGSI conta com o GSI/PR (que o coordena); além dos seguintes órgãos CC/PR; CGU; AGU; SECOM/PR; SG/PR; MJ; MD; MRE; MF; MPS; MS; MDIC; MP; MC; MCTI; MME;

II. **Câmara Multissetorial de SIC e de SegCiber da APF**: câmara consultiva, coordenada pelo GSI/PR, a ser criada em até 90 dias da publicação desta Estratégia, com no máximo 20 instituições, apresentando 55% de representação do Governo, e os demais distribuídos entre academia, setor privado e terceiro setor. A Câmara se reunirá ordinariamente a cada três meses, e extraordinariamente a qualquer tempo.

III. **Conferência de SIC e de SegCiber da APF:** a ser promovida a cada dois anos, como espaço multissetorial e "multistakeholder" de troca de conhecimento e de boas práticas, bem como de promoção da inovação, com representantes do país e do exterior;

IV. **Audiências e Consultas Públicas:** espaços para ampliar o diálogo com a sociedade em nível nacional.

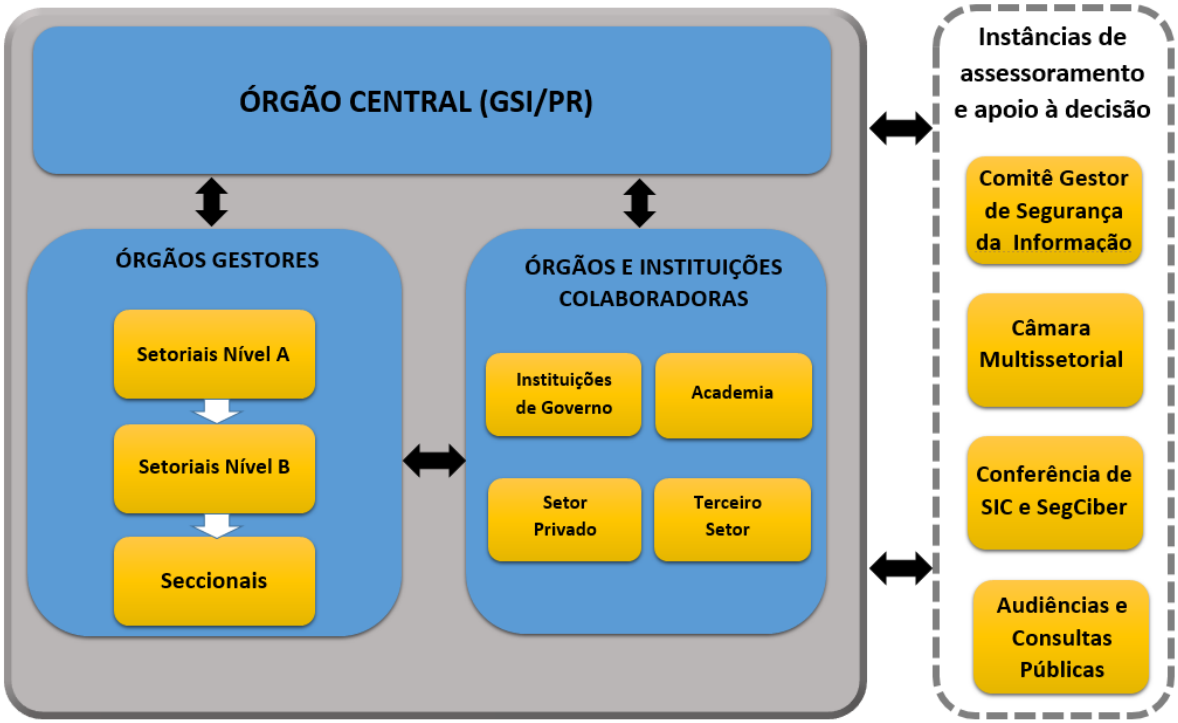


Figura 3 - Modelo de Governança Sistêmica de SIC e de SegCiber da APF

ANEXO II

GLOSSÁRIO DA ESTRATÉGIA

Alta Administração: o termo se aplica às seguintes autoridades públicas: (i) Ministros e Secretários de Estado; (ii) titulares de cargos de natureza especial, secretários-executivos, secretários ou autoridades equivalentes ocupantes de cargo do Grupo-Direção e Assessoramento Superiores - DAS, nível seis; e (iii) presidentes e diretores de agências nacionais, autarquias, inclusive as especiais, fundações mantidas pelo Poder Público, empresas públicas e sociedades de economia mista (Código de Conduta da Alta Administração Federal, 2000).

Ameaça: Conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (NC 04/IN01/DSIC/GSI/PR Rev. 01, 2013).

Artefato malicioso: Qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores (NC 05/IN01/DSIC/GSI/PR, 2009).

Ativo de Informação: Meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (Portaria 45 SE-CDN, 2009; NC 10/IN01/DSIC/GSI/PR, 2012).

Autenticidade: Propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade (IN 01 GSI/PR, 2008).

Balanced Scorecard (BSC): É uma metodologia de gestão de desempenho e de planejamento estratégico (Kaplan e Norton, 1996).

Confidencialidade: Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado (IN 01 GSI/PR, 2008).

Continuidade de Negócios: Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido (NC 06/IN01/DSIC/GSI/PR, 2009).

Defesa: O ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança, ou ainda, reação contra qualquer ataque ou agressão real ou iminente (Glossário MD35-G-01, 2007).

Disponibilidade: Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade (IN 01 GSI/PR, 2008).

Empresa Estratégica de Defesa (EED): Toda pessoa jurídica credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das seguintes condições: (a) ter como finalidade, em seu objeto social, a realização ou condução de atividades de pesquisa, projeto, desenvolvimento, industrialização, prestação dos serviços referidos no art. 10 da Lei nº 12.598/2012, produção, reparo, conservação, revisão, conversão, modernização ou manutenção de PED no País, incluídas a venda e a revenda somente quando integradas às atividades industriais supracitadas; (b) ter no País a sede, a sua administração e o estabelecimento industrial, equiparado a industrial ou prestador de serviço; (c) dispor, no País, de comprovado conhecimento científico ou tecnológico próprio ou complementado por acordos de parceria com Instituição Científica e Tecnológica para realização de atividades conjuntas de pesquisa científica e tecnológica e desenvolvimento de tecnologia, produto ou processo, relacionado à atividade desenvolvida; (d) assegurar, em seus atos constitutivos ou nos atos de seu controlador direto ou indireto, que o conjunto de sócios ou acionistas e grupos de sócios ou acionistas estrangeiros não possam exercer em cada assembleia geral número de votos superior a 2/3 (dois terços) do total de votos que puderem ser exercidos pelos acionistas brasileiros presentes; e (e) assegurar a continuidade produtiva no País (Lei 12.598/2012).

Engenharia Social: Técnica que utiliza o poder de influenciar pessoas visando a quebra de segurança para a obtenção indevida de informação ou para acesso, físico ou lógico, não autorizado (adaptado por: Grupo de Trabalho da Estratégia de SIC e SegCiber da APF, 2015).

Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores (NC 05/IN01/DSIC/GSI/PR, 2009).

Gestão de riscos de segurança da informação e comunicações: Conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos (NC 04/IN01/DSIC/GSI/PR, 2009).

Guerra cibernética: Conjunto de ações para uso ofensivo e defensivo de informações e sistemas de informações para negar, explorar, corromper ou destruir valores do adversário baseados em informações, sistemas de informação e redes de computadores. Estas ações são elaboradas para obtenção de vantagens tanto na área militar quanto na área civil (Glossário MD35-G-01, 2007).

Impacto: Mudança adversa no nível obtido dos objetivos do negócio (ABNT, 2011).

Incidente de segurança: É qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores (NC 05/IN01/DSIC/GSI/PR, 2009).

Infraestruturas Críticas da Informação: Subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (Portaria 34 SE-CDN, 2009; NC 10/IN01/DSIC/GSI/PR, 2012).

Infraestruturas Críticas: Instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (Portaria 45 GSI/PR, 2009).

Nível de Maturidade em SIC e SegCiber: Estágio das práticas de SIC e SegCiber nos órgãos e entidades da APF, baseado em escala, que mede e avalia um conjunto de objetivos que, quando satisfeitos, promovem a melhoria da qualidade na busca da excelência (adaptado por: Grupo de Trabalho da Estratégia de SIC e SegCiber da APF, 2015).

PDCA: *Plan-Do-Check-Act*, metodologia de melhoria contínua referenciada pela norma ABNT NBR ISO/IEC 27001 (NC 02/IN01/DSIC/GSI/PR, 2008).

Quebra de Segurança: Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações (IN 01 GSI/PR, 2008).

Resiliência: Poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre (NC 06/IN01/DSIC/GSI/PR, 2009).

Riscos de segurança da informação e comunicações: Potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização. (NC 04/IN01/DSIC/GSI/PR, 2009).

Segurança Cibernética: Arte de assegurar a existência e a continuidade da Sociedade da Informação de uma Nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas (Portaria 45 SE-CDN, 2009; BRASIL. GSI/PR, 2010).

Segurança da Informação e Comunicações: Ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (IN 01 GSI/PR, 2008).

Segurança da Informação: Proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento (Decreto nº 3.505, 2000).

Tecnologia da Informação e Comunicação (TIC): Recursos necessários para adquirir, processar, armazenar e disseminar informações (NBR ISO/IEC 38500: 2009).

Vulnerabilidade: Propriedade intrínseca de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma conseqüência (ISO 31000, 2009). Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação (NC 04/IN01/DSIC/GSI/PR, 2009).


APF
SIC
SEG CIBER