PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria Executiva
Departamento de Segurança da Informação e Comunicações

GUIA DE REFERÊNCIA PARA A SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO

Versão 01 – Nov./2010

Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior (Organizadores)

Brasília - DF
2010

Presidente da República
Luis Inácio Lula da Silva

Vice-Presidente da República
José Alencar Gomes da Silva

Ministro Chefe do Gabinete de Segurança Institucional
Jorge Armando Felix

Secretário Executivo
Antonio Sérgio Geromel

Diretor do Departamento de Segurança da Informação e Comunicações
Raphael Mandarino Junior

Disponível em formato eletrônico: http://dsic.planalto.gov.br

Organizadores
Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior

Colaboradores
Subgrupos 1, 2 e 3 do Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação – GT SICI
Subgrupo 1: Mapeamento de Ativos de Informação das Infraestruturas Críticas da Informação

Admilson Gonçalves Júnior, Ministério do Planejamento, Orçamento e Gestão
Alexandre Costa Guindani, Caixa Econômica Federal
Alexandre Mariano Feitosa, Ministério da Defesa
José Ney de Oliveira Lima, Ministério do Planejamento, Orçamento e Gestão
Murilo Sérgio de Farias Félix, Petrobras
Núbia Moreira dos Santos, Ministério do Planejamento, Orçamento e Gestão
Pedro André Freire, Serviço Federal de Processamento de Dados
Ricardo Brigatto Salvatore, Ministério da Defesa
Sandro Herman Pereira Rehem, Ministério do Planejamento, Orçamento e Gestão
Suzana de Queiroz Ramos Teixeira, Ministério da Ciência e Tecnologia

Subgrupo 2: Requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: aumentar a segurança, resiliência e capacitação

Amilcar Faria, Banco Central
André Moreira, Banco do Brasil
Danilo Dias, Banco Central
Eduardo Gomes de Barros, Comando do Exército
Humberto Campedelli, Empresa de Tecnologia e Informações da Previdência Social
Marcelo Paiva Fontenele, Comando do Exército
Marcos Allemand Lopes, Serviço Federal de Processamento de Dados

Subgrupo 3: Método para Identificação de Ameaças e Geração de Alertas de Segurança das Infraestruturas Críticas da Informação

Alexandre Hosang, Agência Brasileira de Inteligência
Átila Bandeira, Banco do Brasil
Bernadette S. C. Castilho, Petrobras
João Matos Pinheiro Filho, Agência Brasileira de Inteligência
Paulo Gonçalves Garcia, Ministério das Relações Exteriores

Projeto gráfico, edição e impressão
Agência Brasileira de Inteligência/GSIPR

Apoio de revisão técnica
Marlene Isidro (DSIC/GSIPR)

Ficha Catalográfica
Dados Internacionais de Catalogação na Publicação (CIP)

B823g

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 / Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010.

151 p.
Versão 01

1. Segurança das Infraestruturas críticas da informação – Brasil. 2. Segurança da informação e comunicações - Brasil. 3. Segurança cibernética - Brasil. I. Título. II. Canongia, Claudia. III. Gonçalves Júnior, Admilson. IV. Mandarino Junior, Raphael.

CDD 658.4038
CDU 004.056.57 (035)

Ficha Catalográfica produzida pela Biblioteca da Presidência da República.

Gabinete de Segurança Institucional (GSI/PR)
Secretaria Executiva (SE)
Departamento de Segurança da Informação e Comunicações (DSIC)
Praça dos Três Poderes
Anexo III do Palácio do Planalto. Térreo, Ala A – Sala 107
70150-900 - Brasília, DF
Fax: +55 (61) 3411-1217
Site: http://dsic.planalto.gov.br

APRESENTAÇÃO

É com imensa satisfação que apresento este Guia de Referência, o qual reúne métodos e instrumentos, visando garantir a Segurança das Infraestruturas Críticas da Informação, com relevantes aspectos destacados dada a complexidade do tema nos dias atuais.

Dentre as motivações do Gabinete de Segurança Institucional, órgão essencial da Presidência da República, para esta obra, tem-se a própria prerrogativa do Gabinete de coordenar a atividade de Segurança de Infraestruturas Críticas - definida como as instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional. Assim, motivado por esta missão e considerando a necessidade de assegurar, dentro do espaço cibernético, ações de segurança da informação e comunicações como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação, no âmbito da Administração Pública Federal, direta e indireta; a possibilidade real de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído, em agosto de 2009, um Grupo de Trabalho para estudo e análise de matérias relacionadas à Segurança das Infraestruturas Críticas da Informação - o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade - no âmbito do Comitê Gestor de Segurança da Informação (CGSI).

Este Guia de Referência, além de assistir a missão do GSIPR, reúne estudos técnicos sobre a Segurança das Infraestruturas Críticas da Informação desenvolvidos por especialistas de diferentes órgãos da Administração Pública Federal, direta e indireta. Tal diversidade enriqueceu e propiciou diversas e significativas opiniões sobre o tema, as quais, indubitavelmente, fomentarão discussões e propostas de melhorias sobre o assunto. Dentre os pontos fortes, destaco as recomendações para identificar as interdependências entre os Ativos 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.

Recomendo, portanto, a leitura deste Guia, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução do mesmo, visando estabelecer melhores práticas de Segurança das Infraestruturas Críticas da Informação.

Boa leitura!

Jorge Armando Felix
Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
APF	Administração Pública Federal
BS	*British Standard*
CAIS	Centro de Atendimento a Incidentes de Segurança
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETIR Gov	Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal
CGSI	Comitê Gestor de Segurança da Informação
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
DDoS	*Distributed Denial of Service*
D.O.U.	Diário Oficial da União
DSIC	Departamento de Segurança da Informação e Comunicações
EGTI	Estratégia Geral de Tecnologia da Informação
FISMA	*Federal Information Security Management Act*
GIAC	*Global Information Assurance Certification*
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicações
GSIPR	Gabinete de Segurança Institucional da Presidência da República
GTSIC	Grupo Técnico de Segurança de Infraestruturas Críticas
GTSICI	Grupo de Trabalho de Segurança de Infraestruturas Criticas da Informação
IC	Infraestruturas Críticas
ICI	Infraestruturas Críticas de Informação
ISO	*International Organization for Standardization*
NIST	*National Institute of Standards and Technology*

MPOG	Ministério do Planejamento, Orçamento e Gestão
OWASP	*Open Web Application Security Project*
PDTI	Plano Diretor de Tecnologia da Informação
RNP	Rede Nacional de Ensino e Pesquisa
SICI	Segurança das Infraestruturas Críticas da Informação
SISBIN	Sistema Brasileiro de Inteligência
SISP	Sistema de Administração dos Recursos de Informação e Informática

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

PREFÁCIO

Observamos tendência mundial crescente em destacar e priorizar a elaboração de diretrizes, planos e ações voltados a assegurar e promover a segurança das infraestruturas críticas da informação, em especial pela transversalidade e particularidade do tema.

Entre as justificativas relativas à segurança das infraestruturas críticas da informação, salientamos, a crescente convergência tecnológica, a elevada interconexão de redes e sistemas, e sua interdependência.

No sentido de introduzir tal reflexão no país, o Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação (GT SICI) foi instituído no âmbito do Comitê Gestor de Segurança da Informação (CGSI) com as seguintes atribuições, conforme Portaria Nº. 34 CDN/SE de 05/08/2009[1]:

I - levantar e avaliar as potenciais vulnerabilidades e riscos que possam afetar a Segurança das Infraestruturas Críticas da Informação, o que requer a identificação e monitoramento das interdependências;

II - propor, articular e acompanhar medidas necessárias à Segurança das Infraestruturas Críticas da Informação;

III - estudar, propor e acompanhar a implementação de um sistema de informações que conterá dados atualizados das Infraestruturas Críticas da Informação, para apoio a decisões; e,

IV - pesquisar e propor um método de identificação de alertas e ameaças da Segurança de Infraestruturas Críticas da Informação.

[1] D.O.U. No. 149 de 06/08/2009.

O GT SICI conta com especialistas, designados como titulares e suplentes, de 13 órgãos, a saber: GSIPR/DSIC; Casa Civil/PR; Ministério da Defesa; Ministério das Relações Exteriores; Ministério da Saúde; Ministério do Planejamento, Orçamento e Gestão; Ministério da Ciência e Tecnologia; Banco Central do Brasil; Banco do Brasil; Caixa Econômica Federal; SERPRO, PETROBRÁS, e DATAPREV[2].

O plano de trabalho para o ano de 2010 foi desenvolvido visando oferecer métodos, instrumentos, bem como glossário de conceitos básicos utilizados na Segurança das Infraestruturas Críticas da Informação à comunidade de Segurança da Informação e Comunicações (SIC) e das Infraestruturas Críticas (IEC).

O GT SICI foi, então, subdividido para estudar e desenvolver os seguintes tópicos:

1 - Mapeamento de Ativos de Informação das Infraestruturas Críticas da Informação;

2 - Requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: visando aumentar a segurança, resiliência e capacitação; e,

3 - Método de Identificação de Ameaças e Geração de Alertas de Segurança das Infraestruturas Críticas da Informação.

Os três subgrupos contaram com participação efetiva de membros titulares, suplentes, bem como de convidados do citado GT SICI, e os estudos foram desenvolvidos de março a setembro de 2010, por meio de reuniões presenciais e virtuais.

Os estudos desenvolvidos expressam significativa e substantiva colaboração técnica, calcadas em múltiplas visões da Administração Pública Federal, direta e indireta, e abrem espaço para observações e sugestões de melhorias adicionais e contínuas, caracterizando-se como importante

[2] Portaria No. 59 publicada no D.O.U No. 215 de 11/11/2009.

subsídio para a elaboração do “Plano de Segurança das Infraestruturas Críticas da Informação” do País.

Como ponto de partida, os seguintes conceitos balizaram os estudos e trabalhos iniciais do GT SICI: “Infraestruturas Críticas da Informação”, como o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade; e, complementarmente, “Ativos de Informação” como 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.

Ao término dos trabalhos, os Subgrupos apresentaram suas propostas à Coordenação do GT, exercida pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR), por intermédio de seu Departamento de Segurança da Informação e Comunicações (DSIC), a qual, diante da excelência das propostas apresentadas, levou à consideração do Comitê Gestor de Segurança da Informação (CGSI) a proposição de publicação de um livro que consolidasse os trabalhos, o que permitiu a geração do “Guia de Referência para a Segurança das Infraestruturas Críticas da Informação”, como subsídio técnico de extrema importância aos gestores de segurança da informação e comunicações bem como aos gestores de infraestruturas críticas.

São destacados, a seguir, os tópicos principais tratados no livro:

- ✓ Introdução: apresenta, além da caracterização e contextualização do tema segurança das infraestruturas críticas da informação, sistemática para avaliação de riscos com proposta mais detalhada de gerenciamento de riscos e continuidade de negócios;

- ✓ Capítulo 1: apresenta os ***"Macroprocessos de Mapeamento de Ativos de Informação***", no intuito de delinear caminhos para determinar se um ambiente é ou não seguro no que se refere à informação e comunicações, considerando-se a DICA (critérios de Disponibilidade, Integridade, Confidencialidade e Autenticidade). Somam-se questões relativas à crescente incidência de ataques cibernéticos, o que torna ainda maior a necessidade de rastrear interdependências internas/externas, a fim de que sejam identificados os impactos decorrentes da interrupção dos serviços oriundos de infraestruturas críticas da informação, e que sejam implementadas ações adequadas à manutenção da continuidade dos serviços. Uma das principais medidas iniciais refere-se ao alcance do entendimento inequívoco dos ativos de informação, e também da identificação de seus respectivos contêineres;
- ✓ Capítulo 2: propicia "***Instrumentos para o Mapeamento e o Acompanhamento de Ativos de Informação"***, contempla tanto um questionário, com 50 questões fechadas, quanto um conjunto de formulários que objetivam facilitar a identificação, registro, e gestão dos ativos de informação. Além de disponibilizar anexos que oferecem Lista de ameaças comuns, segundo Norma ABNT (2008a), Lista de vulnerabilidades, também baseada na Norma ABNT (2008a), e, Tabelas de caracterização dos perfis das ameaças;
- ✓ Capítulo 3: apresenta modelo e instrumentos de apoio a gestão e

acompanhamento de "***Requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: aumentar a segurança, resiliência e capacitação"*** , por meio da categorização dos controles e respectivos itens de controles de segurança da informação e comunicações, de forma a atender aos requisitos mínimos de segurança das infraestruturas críticas da informação, e, também, visando permitir a identificação e o acompanhamento do nível de maturidade da segurança das infraestruturas críticas da informação nas organizações. O modelo e instrumentos tomaram como base a legislação brasileira vigente sobre o tema, bem como referencial normativo internacional, tais como NIST, ISO, FISMA, GIAC, OWASP, e a experiência do Centro de Controle da Coréia do Sul, o qual aplica como metodologia de trabalho para este tema, categorias de controle e níveis de maturidade. Além disso, este Capítulo demonstra o alinhamento e a respectiva correspondência dos itens de controles propostos com a identificação dos ativos de informação, conforme o questionário apresentado no Capítulo 2. Soma-se que para a construção de visão sistemática e de evolução continuada foram estabelecidas camadas em cinco níveis de maturidade, sendo estes transpostos em ciclos até que o órgão / instituição atinja o nível mais elevado de maturidade, propondo-se o nível 2 como nível mínimo de maturidade inicial em Segurança das Infraestruturas Críticas da Informação. Há um reforço adicional do trabalho ao utilizar os

conceitos de proteção – resiliência – segurança; passando-se pelos conceitos de resiliência operacional, condição prévia para se atingir a resiliência organizacional;

- ✓ Capítulo 4: indica "***Método para Identificação de Ameaças e Geração de Alertas de Segurança das Infraestruturas Críticas da Informação"***, busca nortear as ações a partir dos princípios da seletividade e da oportunidade, para a geração de alertas, por meio de processo que compreende ações de coleta – análise – divulgação, a serem realizadas pelos responsáveis (gestores das Infraestruturas Críticas da Informação – ICI). As ações contribuirão para a formação de uma rede de colaboração e comunicação, que poderá ser coordenada de forma centralizada, descentralizada, ou híbrida, e cuja finalidade principal é a troca de sinais (ameaças ainda não validadas, mas que precisam ser comunicadas). Essa sinalização deve ser controlada por um setor específico para que sejam tomadas as medidas adequadas de resposta aos alertas. Ao final deste Capítulo, descreve-se o ***Módulo de Monitoramento de Ameaças e Geração de Alertas de Segurança das Infraestruturas Críticas da informação***, que foi desenvolvido baseado no mapeamento dos ativos de informação e respectivos itens de controle, promovendo, assim, o alinhamento e a sinergia com os 3 Capítulos deste livro, no sentido de fomentar a visão ora proposta do Guia de Referência para a Segurança das Infraestruturas Críticas da Informação.

A Coordenação do GT SICI muito tem a agradecer aos titulares, suplentes e colaboradores convidados do GT, dado o empenho, a dedicação, e a colaboração de excelência técnica de todos, o que permitiu organizar e lançar este Guia.

Achamos que vale dizer também que durante as reuniões ordinárias do GT SICI, bem como por meio eletrônico, a Coordenação do GT colaborou intensa e sistematicamente com os rumos e objetivos que os estudos deveriam seguir, sem contudo, interferir diretamente na proposição técnica dos especialistas colaboradores, estimulando a construção de novos conhecimentos no tema.

Finalmente, sabemos que este é o primeiro passo, e que muito há ainda por construir. Por isso, queremos convidá-lo a contribuir com os avanços deste Guia, registrando seu relato de experiência de segurança das infraestruturas críticas da informação, no Portal do DSIC[3]. Sua participação certamente ampliará nosso conhecimento e permitirá inovar os modelos, instrumentos, e conceitos deste Guia.

Raphael Mandarino Junior
Coordenador do GT SICI
Diretor do DSIC/GSIPR

Claudia Canongia, Dra.
Representante suplente do GSIPR no GT SICI
Assessora Técnica do DSIC/GSIPR

[3] https://dsic.planalto.gov.br/fale-com-o-dsic

INTRODUÇÃO

As Infraestruturas Críticas (IC) - instalações, serviços, bens e sistemas – exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não. Ao passar dos anos, a interdependências verticais das Infraestruturas Críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões (BAGHERY, 2007).

Na prática, com a ausência da operação apropriada de uma IC, a função de outras poderiam ser interrompidas, provocando sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade (CDN/SE, 2009).

As áreas prioritárias das Infraestruturas Críticas, sem prejuízo de outras que porventura vierem a ser definidas, são expressas nos incisos de I a V do art. 3º da Portaria Nº 02 do Gabinete de Segurança Institucional da Presidência da República, de 8 de fevereiro de 2008. São elas, respectivamente conforme mencionadas na Portaria: Energia, Transporte, Água, Telecomunicações e Finanças. A mesma Portaria instituiu os Grupos Técnicos de Segurança das Infraestruturas Críticas (GTSIC), com a finalidade de que aqueles proponham a implementação de medidas e ações relacionadas com a segurança destas.

Os serviços prestados por essas áreas são de vital importância para os cidadãos, para as organizações e para o

Estado, cuja proteção permanente visa garantir a continuidade da prestação dos serviços mesmo em situações de crise.

As Infraestruturas Críticas da Informação (ICI) são assim definidas como o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (CDN/SE, 2009).

As Infraestruturas Críticas de Informação possuem a peculiar característica de poderem fazer parte, com relações de interdependências horizontais, de várias Infraestruturas Críticas, ou seja, a informação gerada por determinada área prioritária das Infraestruturas Críticas pode ser insumo para outra, evidenciando, desta forma, o alto grau de acoplamento e interdependência existente entre elas.

Tal fato eleva a necessidade da identificação dos ativos de informação essenciais, bem como o tratamento dos riscos a que estes ativos estão expostos, pois o impacto causado pela perda ou indisponibilidade destes ativos pode comprometer toda a cadeia de Infraestruturas Críticas existentes.

Os Ativos de Informação, como qualquer outro relevante para o negócio, tem valor para a organização e necessita ser adequadamente protegido. Além disso, as dependências dos sistemas e serviços, as tendências e evoluções tecnológicas da computação distribuída, as interconexões de redes públicas e privadas e o compartilhamento de recursos expõem as organizações às diversas ameaças, entre elas: fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo, inundação, *blackouts*, códigos maliciosos, *hackers*, ataques de *DDoS*, entre outras (ABNT, 2005).

Segundo a ABNT (2005), Segurança da Informação[4] (SI), como parte integrante do processo global de Gestão de Segurança, tem como objetivo proteger a informação contra ameaças no intuito de garantir a continuidade, minimizar os danos e maximizar os investimentos e oportunidades do negócio. A segurança da informação é obtida com a utilização de controles: políticas, práticas, procedimento, estruturas organizacionais e infraestruturas de *hardware* e *software*. É caracterizada pela preservação da disponibilidade, integridade, confidencialidade e autenticidade da informação, e visa preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização. Mais recentemente, a **Instrução Normativa Nº 1 GSIPR (2008b)** define a **Segurança da Informação e Comunicações** como ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Adicionalmente, conta-se com a Instrução Normativa Nº 4 SLTI/MPOG (2008) que dispõe sobre o processo de contratação de serviços de tecnologia da informação pela Administração Pública Federal direta, autárquica e fundacional. Soma-se que a Estratégia Geral de Tecnologia da Informação (EGTI) para a APF, revisada anualmente, subsidia a elaboração dos Planos Diretores de Tecnologia da Informação (PDTI) dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Informação e Informática (SISP)[5].

[4] No País, o Decreto Nº 3.505, de 13 de junho de 2000, e o Decreto Nº 4.553, de 27 de dezembro de 2002, dispõem respectivamente, no âmbito da Administração Pública Federal, direta e indireta: pela instituição da Política de Segurança da Informação nos órgãos e entidades; e sobre a salvaguarda de dados, informações, documentos e materiais classificados de interesse da segurança da sociedade e do Estado.

[5] O Ministério do Planejamento, Orçamento e Gestão é o órgão central do SISP e, nesta condição, interage com o Gabinete de Segurança Institucional da Presidência da República (GSIPR) para a divulgação e implementação da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

Para que uma organização identifique seus requisitos de segurança, ela deve basear-se em três pilares. O primeiro é o conjunto dos princípios, objetivos e necessidades para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações. O segundo é a legislação vigente, os estatutos, as regulamentações e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender. E o terceiro, oriunda das duas anteriores, são os requisitos de segurança derivados da avaliação de riscos, processo responsável por identificar as ameaças aos ativos, as vulnerabilidades com suas respectivas probabilidades de ocorrência e os impactos ao negócio.

Organizações de todos os tipos e tamanhos enfrentam influências e fatores internos e externos que tornam incerto se e quando serão atingidos os objetivos. O efeito dessa incerteza sobre os objetivos da organização é o que chamamos de risco (ABNT, 2009a).

Ainda conforme a Norma, todas as atividades de uma organização envolvem risco. As organizações que gerenciam o risco buscam identificar, analisar, avaliar e tratar os riscos identificados, a fim de atender aos critérios e requisitos necessários a continuidade de suas operações.

A Gestão de Riscos (GR) quando implementada e mantida possibilita a uma organização ou a uma IC:

a) Aumentar a probabilidade de atingir seus objetivos;
b) Encorajar a gestão pró-ativa;
c) Identificar e tratar os riscos através de toda a organização;
d) Melhorar a governança;

e) Melhorar os controles;

f) Melhorar a eficácia e eficiência operacional;

g) Minimizar perdas;

h) Aumentar a resiliência da organização.

Desta forma o processo de Gestão de Riscos produzirá subsídios para suportar o Sistema de Gestão de Segurança da Informação e Comunicações e a Gestão de Continuidade dos Negócios.

Definir o escopo de aplicação da Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC é, portanto, necessário a fim de delimitar seu âmbito de atuação. Esse escopo pode abranger o órgão ou entidade como um todo, um segmento, um processo, um sistema, um recurso ou um ativo de informação, segundo leciona a Norma Complementar Nº 04/IN01/DSIC/GSIPR (2009a).

No caso da Infraestrutura Crítica da Informação, o escopo de aplicação dos conceitos e métodos de GRSIC é o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso – que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (CDN/SE, 2009).

Existe certa complexidade no estabelecimento de parâmetros que sirvam de subsídio para a afirmação de que um ambiente de informação é seguro. É importante a identificação das consequências relacionadas às vulnerabilidades do tratamento da informação, da compreensão dos diversos ambientes de contexto e da adoção de um modelo de segurança que possa minimizar tais consequências (CT-STI, 2000).

Considerando esses aspectos, as ameaças à segurança da informação se concentram em dois pontos: as vulnerabilidades existentes nos ambientes onde a informação é processada, armazenada ou transmitida e as ameaças externas e internas à segurança da informação nestes ambientes (CT-STI, 2000).

Independentemente destas definições entende-se que a GRSIC, aplicada a ICI, deve abranger, no mínimo, as seguintes ameaças potenciais:

a) Terremotos
b) Furações
c) Tornados
d) Inundação
e) Falta de Energia
f) Problemas no Transporte Público
g) Greves
h) Pandemias
i) Escândalos
j) Vazamento de Informações
k) Incêndios
l) Contaminação Química
m) Distúrbios Sociais
n) Bombas
o) Terrorismo
p) Falhas de Hardware
q) Falhas de Software
r) Vírus e *worms*
s) Morte de Pessoa Chave

Importante destacar que por melhor que seja o processo de GRSIC implementado em uma ICI ele tem caráter apenas preventivo, não evitando que os riscos se concretizem, apenas possibilitando a redução das probabilidades de ocorrência.

Segundo a Norma Complementar Nº 04/IN01/DSIC/GSIPR (2009a), o processo Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC tem como objetivo manter os riscos, a que os ativos de informação estão expostos, em níveis aceitáveis.

Esse processo de gestão é composto pelas etapas de definições preliminares, análise/avaliação dos riscos, plano de tratamento dos riscos, aceitação dos riscos, implementação do plano de tratamento dos riscos, monitoração e análise

crítica, comunicação do risco, alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), definido na Norma Complementar Nº 02/IN01/DSIC/GSIPR (2008c), de modo a fomentar a sua melhoria contínua.

As etapas que compõem o ciclo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) são apresentadas na figura abaixo:

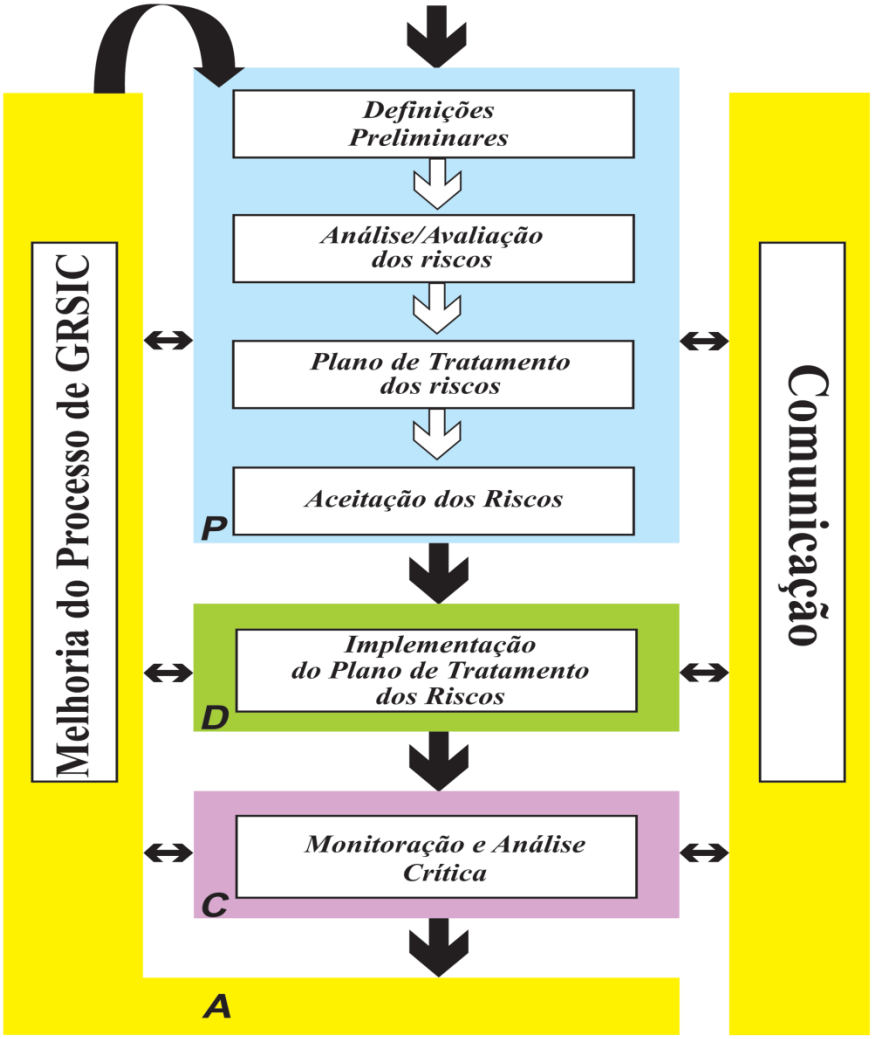


Figura 0.1 - Ciclo da Gestão de Riscos de Segurança da Informação e Comunicações (GSIPR, 2009a)

Além do exposto, para que uma Infraestrutura Crítica (IC) esteja protegida de forma adequada é necessário que se implemente um processo de gestão abrangente que identifique as ameaças potenciais e os possíveis impactos aos seus ativos, processos ou pessoas, caso estas ameaças se concretizem.

Este processo de gestão fornecerá uma estrutura para o desenvolvimento de resiliência da IC, conferindo a capacidade de responder efetivamente a um evento ou interrupção e salvaguardar os interesses do Estado e a segurança da sociedade, por meio da recuperação da IC afetada.

Com base nessa definição podemos dizer que a Gestão de Continuidade de Negócio (GCN) busca preparar a Infraestrutura Crítica para responder a eventos que possam provocar uma interrupção significativa em suas atividades essenciais, o que colocaria em risco sua sobrevivência.

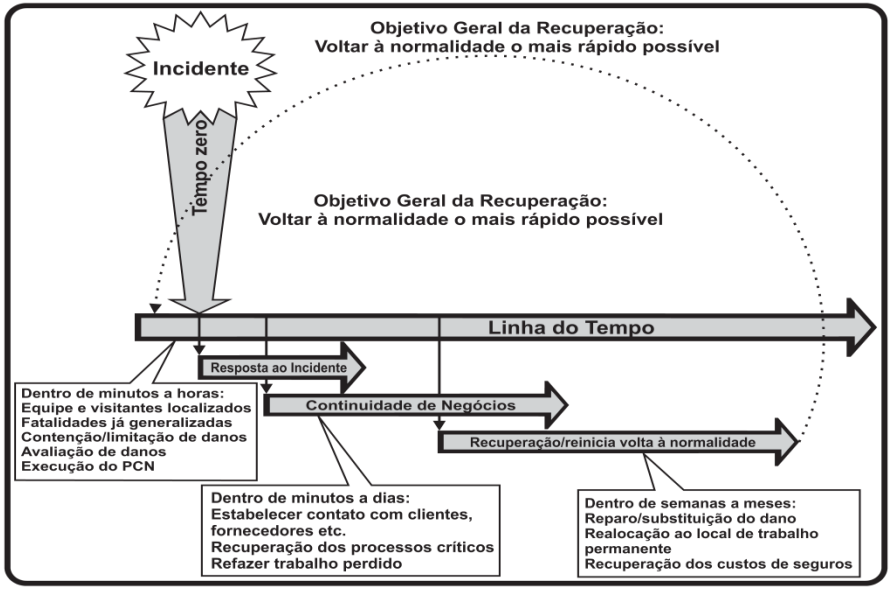


Figura 0.2 - Processo de Gestão da Segurança da Informação

O conceito e a metodologia da GCN, consolidada pelas normas BS 25999, NBR 15999 e pela Norma Complementar Nº 06/IN01/DSIC/GSIPR (2009c), são indicadas para a

proteção das Infraestrutura Crítica priorizadas pela Portaria Nº 02 do Gabinete de Segurança Institucional da Presidência da República, de 8 de fevereiro de 2008.

De forma resumida podemos dizer que a implementação da GCN possibilitará:

a) Entender os requisitos e as necessidades da IC;
b) Desenvolver e implementar estratégias de continuidade adequadas aos requisitos da IC;
c) Capacitar a Infraestrutura Crítica para responder adequadamente a incidentes, emergências e crises de qualquer natureza;
d) Desenvolver planos;
e) Testar e manter atualizados esses planos;
f) Educar todos os servidores/empregados envolvidos na recuperação da IC.

A necessidade de assegurar dentro do espaço físico ou cibernético ações de segurança da informação como fundamentais para garantir disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações no âmbito da Administração Pública Federal, direta e indireta; a possibilidade real de uso dos meios computacionais para ações ofensivas através da penetração nas redes de computadores de alvos estratégicos; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade (CDN/SE, 2009), motivam a confecção deste Guia, cujo objetivo é auxiliar tanto os gestores de Segurança da Informação quanto os de Infraestruturas Críticas a identificar e a mapear os ativos de informação, considerando suas interdependências – internas e externas à organização - e potenciais vulnerabilidades e riscos que possam afetar a segurança de Infraestruturas Críticas da Informação.

CAPÍTULO 1. MACROPROCESSOS PARA MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

O Mapeamento de Ativos de Informação é um processo iterativo e evolutivo, composto por três atividades: **(1) identificação e classificação de ativos de informação**, **(2) identificação de potenciais ameaças e vulnerabilidades** e **(3) avaliação de riscos**.

O produto de cada atividade servirá de insumo para as atividades subsequentes, e o resultado final do processo deverá proporcionar à Alta Administração condições para priorizar quais ativos de informações deverão receber ações de controle, visando o tratamento de riscos para a redução dos impactos ao negócio. Além disso, o produto final do processo irá subsidiar as atividades de **identificação e classificação de ativos de informação** e **identificação de potenciais ameaças e vulnerabilidades** quando um novo ciclo do processo for executado.

Recomenda-se como boa prática a revisão de todo o processo periodicamente, e pontualmente quando um novo ativo de informação é agregado ao inventário. Também são considerados como boas práticas: testar periodicamente os controles de riscos implantados; e registrar eventos de incidentes de segurança em uma base de conhecimento, a qual deve constar, pelo menos, a identificação do ativo de informação, o incidente, a solução de contorno, a causa raiz e a solução definitiva.

A seguir é apresentada a sequência de atividades do processo e os possíveis produtos de cada uma:

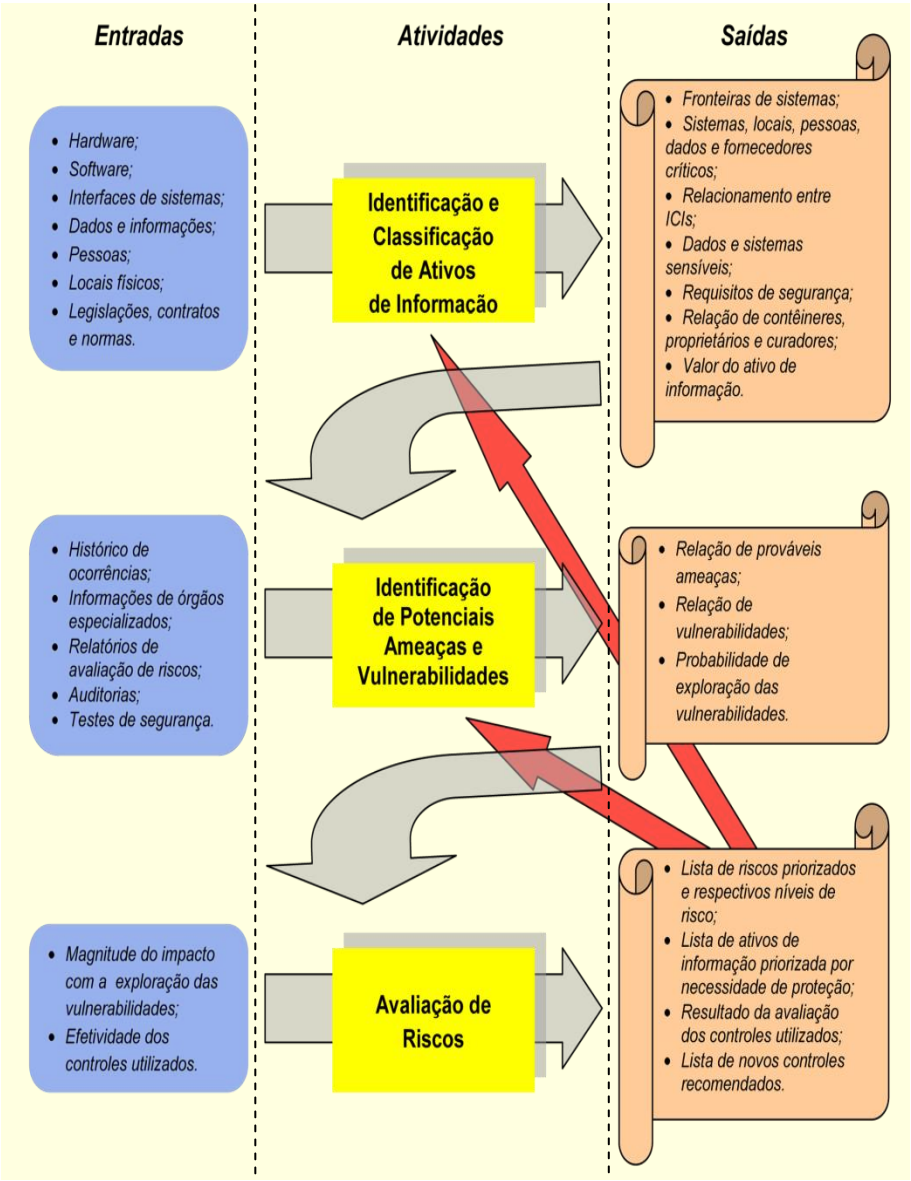


Figura 1.1 - Macroprocessos do Mapeamento de Ativos de Informação

Convém que a condução das atividades do processo seja realizada sob o viés de cinco perspectivas, as quais visam fornecer uma visão macro a respeito dos impactos que

a ausência da operação apropriada desses ativos poderá causar às Infraestruturas Críticas da Informação. As perspectivas propostas são: Social, sob os aspectos de Saúde, Abastecimento e Meio Ambiente; Econômica; Política; Internacional; e, Segurança do Estado e da Sociedade. Abaixo, segue maior detalhamento a respeito de cada perspectiva e como o processo deverá ser direcionado:

1) **Social:**
   a) **Saúde**: relacionada à saúde da sociedade. Quão importante é o ativo de informação para manter a saúde e o bem-estar da população atendida por ele? Caso a segurança desse ativo seja comprometida, as pessoas poderão sofrer danos físicos ou mentais?
   b) **Abastecimento**: relacionada ao abastecimento de bens e serviços próprios para a sociedade, como água, energia, transporte, telecomunicações, entre outros. Caso o ativo de informação tenha algum requisito de segurança comprometido, poderão ocorrer problemas de abastecimento?
   c) **Meio Ambiente**: relacionada ao ambiente em que o ativo de informação se insere. Caso um ou mais requisitos de segurança não sejam atendidos, haverá danos ao meio ambiente?
2) **Econômica**: relacionadas à estabilidade econômica e financeira do País e de seus Estados e Municípios. Caso o ativo de informação tenha sua segurança prejudicada, a economia local sofrerá algum impacto?
3) **Política**: relacionada ao cenário político da localidade onde o ativo se encontra. Haverá problemas políticos caso a segurança do ativo de informação seja comprometida?
4) **Internacional**: relacionada às relações internacionais do País e à interdependência do ativo de informação

com ativos de outros países. O comprometimento da segurança do ativo pode impactar na soberania nacional, resultar em problemas para outros países ou no relacionamento do Brasil com o ambiente internacional?

5) **Segurança do Estado e da Sociedade**: relacionada à garantia do nível de segurança ideal para o Estado e para a sociedade. Caso a segurança do ativo seja comprometida, haverá impacto para a segurança do Estado e da sociedade?

1.1. Identificação e Classificação de Ativos de Informação

O crescente incremento da complexidade técnica e ambiental dos negócios representa grandes obstáculos e desafios para aqueles necessitam proteger seus ativos de informação. Esses ativos, por sua vez, sofrem constantes processamentos e combinações, gerando outros recursos cada vez mais complexos e inter-relacionados. É tênue a linha entre posse e custódia dos recursos de informação, pois a informação flui livremente por toda a organização e frequentemente ultrapassa suas fronteiras chegando a outros atores, como: colaboradores, clientes, fornecedores e concorrentes. O processo de Identificação e Classificação de Ativos de Informação auxilia a organização a conhecer, valorizar, proteger e manter seus recursos em conformidade com os requisitos legais e do negócio.

O processo de Identificação e Classificação de Ativos de Informação tem como objetivos prover à organização: um entendimento comum, consistente e inequívoco das fronteiras dos ativos; a identificação clara de seu(s) proprietário(s); um conjunto completo de informações sobre os requisitos de

segurança de cada recurso; uma descrição de onde o bem está contido, é processado e é transportado; e a identificação do valor que o ativo representa para o negócio. Por fim, o processo cria condições para que os *stakeholders* possam desenvolver e aplicar planos de gerenciamento de riscos sobre tais ativos, em conformidade com os requisitos legais e organizacionais (STEVENS, 2005).

1.1.1. Metodologia

O processo de Identificação e Classificação de Ativos de Informação é composto por seis atividades: **(1) coletar informações gerais**; **(2) definir as informações dos ativos**; **(3) identificar o(s) responsável(is)**; **(4) identificar os contêineres dos ativos**; (**5) definir os requisitos de segurança**; e **(6) estabelecer o valor do ativo de informação**. Cada atividade do processo coleta informações adicionais sobre os recursos, as quais podem ser refinadas conforme novas percepções identificadas nas atividades seguintes. Quando isto acontece, o processo dever ser reiniciado com cada ativo de informação para garantir acuracidade e consistência entre as atividades (STEVENS, 2005).

Atividade 1 - Coletar Informações Gerais

O objetivo desta atividade é definir como será a estratégia da coleta das informações, quem serão os responsáveis e qual a previsão de conclusão dos trabalhos.

É natural que os recursos da informação evoluam com o tempo, desta maneira, os perfis gerados pelo mapeamento dos ativos da informação precisam ser constantemente atualizados ou até mesmo recriados. Além disto, pode ser necessário investigar ou saber a história de um ativo (STEVENS, 2005).

Segundo o autor, especificar o quando e por quem foi gerado o mapeamento do ativo garante melhor processo de continuidade e conhecimento sobre este recurso. Como no caso da Alta Direção poder solicitar uma avaliação nas mudanças significativas de posse, de custódia ou no valor do recurso dentro da organização.

Atividade 2 – Definir as informações dos ativos

A finalidade desta etapa é caracterizar o escopo da atividade de mapeamento, ou seja, antes de se executar qualquer tarefa, a organização deve compreender e concordar quais ativos serão considerados e qual o nível de profundidade das informações coletadas.

O nível de detalhe das informações dos ativos, definido pela organização a partir da necessidade do negócio, deve ser suficiente para determinar o conteúdo do recurso, suas fronteiras, o(s) responsável(is), o valor e os requisitos de segurança. Nestes casos, utilizar o bom senso e ser consistente na definição dos ativos ajuda a reduzir a complexidade na coleta das informações.

A definição do recurso da informação deve esforçar-se para satisfazer exigências mínimas de: **consistência** (não muda durante curtos períodos de tempo); **clareza** (não é ambígua ou vaga, sujeitando a dupla interpretação); **entendimento universal** (está acima de linguagens e tecnologias); **aceitação** (é aceitável conforme requisitos do negócio); **materialidade** (é clara a respeito de como o recurso é fisicamente instanciado - papel, mídia magnética, etc.) (STEVENS, 2005).

É importante, quando possível, envolver o proprietário do recurso e outras partes interessadas no processo da definição. Isso assegurará a exatidão e a consistência da definição e da aceitação da atividade. Em alguns casos o proprietário não poderá ser determinado até que o recurso

seja totalmente definido. Nestes casos, a definição do recurso da informação deve ser revista com o proprietário após este for identificado na atividade 3.

Atividade 3 – Identificar o(s) responsável(is)

A atividade 3 é uma das mais importantes da metodologia, pois é nela que o(s) responsável(is) será(ão) definido(s). O proprietário irá acompanhar e validar o restante do processo de Identificação e Classificação de Ativos de Informação.

Identificar a posse de um ativo da informação tem influência direta na eficácia da segurança e na gestão de riscos dos recursos da informação. Grande parte das organizações se isenta de realizar um inventário exato e completo de seus recursos. A falha na identificação dos proprietários do recurso é uma das razões preliminares pelas quais a gerência da segurança da informação é frequentemente ineficaz.

O proprietário de um ativo da informação deve ser uma parte interessada da organização, legalmente instituído, responsável por (STEVENS, 2005):

- Descrever o recurso da informação, conforme atividade 2;
- Definir as exigências de segurança do recurso da informação, conforme atividade 5;
- Comunicar as exigências de segurança do recurso da informação a todos os curadores e usuários;
- Assegurar-se de que as exigências da segurança estejam cumpridas através de monitoramento;
- Projetar uma estratégia apropriada de proteção do ativo da informação;

- Determinar os riscos que possam afetar os ativos de informação;
- Desenvolver as estratégias de tratamento de riscos.

A definição da posse de um ativo da informação deve ter foco no papel ou na posição do proprietário dentro da organização e não em uma pessoa específica. Segundo o autor, trocam-se as pessoas, mas as posições permanecem.

Atividade 4 – Identificar os contêineres dos recursos

A finalidade desta etapa é capturar uma lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado e quem são os responsáveis por manter estes recipientes. Além disso, define os limites do ambiente que deve ser examinado para o risco e igualmente descreve os relacionamentos que devem ser compreendidos para exigências de segurança. Pode ser executada paralelamente à atividade 3, porque não há nenhuma dependência entre as duas atividades.

Num processo de avaliação de riscos, a identificação dos contêineres é essencial para identificar os riscos associados à informação. Os ativos de informação são protegidos a partir dos controles implementados nos seus respectivos contêineres, ou seja, o nível de proteção fornecido pelos controles relaciona-se diretamente com a efetividade ao atendimento dos requisitos de segurança do ativo de informação. O ativo de informação herda os riscos aos quais seus contêineres estão sujeitos. De maneira geral, os contêineres podem ser subdivididos em quatro categorias (STEVENS, 2005):

- Sistemas e aplicações;
- Hardwares;
- Pessoas;

- Outros.

O autor propõe algumas questões básicas que podem ser úteis para identificar contêineres:

- Qual sistema de informação ou aplicação usa ou processa determinada informação?
- Em quais plataformas os ativos de informação podem ser encontrados?
- Que pessoas têm acesso à informação? Essas pessoas podem ser agrupadas?
- Algum processo automático depende do recurso da informação?
- Que tipos de mídias são utilizados para armazenar a informação?
- A informação é frequentemente impressa, quem pode imprimi-la e onde as cópias impressas são armazenadas?
- Cliente e parceiros têm acesso à informação?
- Há cópias de segurança externas contratadas por terceiros?
- Há locais onde a informação possa ser armazenada fisicamente (papel, mídias magnéticas, etc.)?

Atividade 5 – Definir os requisitos de segurança

Nesta atividade, os requisitos de segurança da informação devem ser definidos por meio de critérios que atendam a disponibilidade, integridade, confidencialidade e autenticidade dessa informação. Se um proprietário de um ativo da informação não for capaz de apropriadamente definir os requisitos de segurança desse ativo, não poderá existir e garantir que o curador possa efetivamente protegê-lo.

Podem ser fontes primárias de requisitos de segurança: acordos, contratos, leis, relacionamento com

outros ativos de informação, expectativas das partes interessadas e exigências do negócio.

Atividade 6 – Estabelecer o valor do ativo da informação

Antes que os riscos de um ativo da informação possam ser devidamente avaliados, um valor, tangível ou não, deve ser determinado ao ativo.

O proprietário do ativo da informação e as partes interessadas devem determinar o valor do ativo para o negócio. O valor do ativo deve refletir o quão ele é importante para a organização alcance seus objetivos, em outras palavras, quão impactante será sua indisponibilidade. Normalmente o valor do ativo da informação não está nele mesmo, mas no processo de negócio que ele suporta (STEVENS, 2005).

O valor do ativo será útil para a alta administração decidir a respeito, através de uma análise de custo e benefício, dos controles que devem ser utilizados para mantê-lo.

1.1.2. Fronteiras dos Ativos de Informação

A informação pode ser entendida como a comunicação da inteligência ou do conhecimento do negócio. Os dados – elementos utilizados como insumos para cálculos, discussões e raciocínios – são componentes essenciais da informação. A transformação dos dados em informação ocorre da necessidade da organização em mesclar tais dados num certo contexto, o qual agrega valor.

O contínuo ciclo que move os dados através do processo de criar novas informações resulta no desafio de determinar os limites dos recursos de informação. Utilizando o viés da Segurança da Informação e Comunicações, a

determinação de novos requisitos de segurança pode despertar os seguintes questionamentos, segundo STEVENS (2005):

- O novo ativo de informação é substancialmente diferente daqueles os quais lhe deram origem? Em outras palavras, é realmente “novo”?
- Quem é o proprietário do novo recurso? É o mesmo dos recursos originários ou não?
- Quais são os requisitos de segurança do novo recurso de informação? A simples combinação dos requisitos de segurança dos ativos originários é suficiente para manter o novo ativo ou é necessário definir um novo conjunto? Os novos ativos requerem tratamento mais detalhado ou mais simplificado do que os ativos anteriores?

Com a definição clara dos limites de um ativo de informação, a organização pode determinar requisitos de unicidade, posse e segurança. Além de estabelecer, com melhor exatidão, o valor desse ativo.

1.1.3. Contêineres dos Ativos de Informação

O contêiner é o local onde “vive” o recurso de informação. Geralmente o contêiner descreve o tipo da tecnologia - hardware, software, um sistema de informação - ou até mesmo pessoas, papéis ou mídias magnéticas. Em outras palavras, **o contêiner é qualquer tipo de recurso onde a informação está armazenada, é transportada ou processada** (STEVENS, 2005).

Há três pontos importantes a respeito da segurança e do conceito de contêineres:

- A proteção e a segurança do ativo de informação depende do nível de controle implementado no contêiner;
- O grau de proteção e segurança do ativo depende da eficácia dos controles implementados no contêiner e o quanto tais controles são alinhados com os requisitos exigidos pelo ativo;

- O ativo de informação herda quaisquer riscos os quais está sujeito seu contêiner. Desta forma, quando se avalia riscos para um recurso de informação, as vulnerabilidades de seu contêiner devem ser consideradas.

1.1.4. Propriedade e Custódia dos Ativos de Informação

Proprietários

Os proprietários dos ativos de informação são os responsáveis primários pela viabilidade e sobrevivência dos ativos. Já o curador refere-se a qualquer indivíduo que tem responsabilidade de proteger um recurso de informação, como ele é armazenado, transportado e processado (STEVENS, 2005).

São os proprietários dos recursos os responsáveis por definir os requisitos de segurança e comunicar os curadores a respeito desses requisitos. Aos proprietários incumbe-se também determinar, periodicamente, a eficácia da metodologia de controle sobre as exigências de segurança.

Conforme STEVENS (2005), além de definir e comunicar os requisitos de segurança, os proprietários dos recursos de informação são responsáveis por:

- Definir o escopo do ativo de informação. Normalmente, a definição dos limites não fornece resultados claros, devido à subjetividade que determinados recursos podem apresentar. Cabe ao proprietário desenvolver uma definição do recurso que pode consistentemente ser aplicado por curadores e também por usuários;
- Estabelecer um valor (monetário ou não) do ativo. O valor do ativo de informação é subsídio

para determinar a importância e a criticidade do recurso para a organização e para direcionar uma estratégia apropriada de mitigação de riscos, com controles que justificam uma aceitável relação entre custos e benefícios.

Um proprietário pode delegar a responsabilidade de definir as exigências de segurança, mas não pode abrir mão da responsabilidade sobre a proteção do recurso. Uma vez identificados os proprietários, a organização pode começar a exigir deles o cumprimento de suas obrigações em relação à manutenção dos ativos de informação.

Curadores

Os curadores dos ativos de informação controlam ou são responsáveis pelos contêineres. O termo curador implica num relacionamento próximo entre ele o recurso de informação. Desta forma, ele aceita a responsabilidade de garantir a proteção do recurso, sendo confundido muitas vezes com o proprietário (STEVENS, 2005).

Tipicamente, custódia é considerada em termos de administrador ou gerente de segurança da informação e comunicações, cuja responsabilidade de guardar os ativos de informação compõe o rol de tarefas para manter os processos de negócio da organização, e inclui necessariamente um esforço colaborativo com os gestores de TI.

Há três pontos importantes a respeito da relação entre curadores e ativos de informação, levantados por STEVENS (2005):

- De posse dos ativos de informação, ou de seus respectivos contêineres, os curadores são responsáveis por aplicar os níveis os controles de segurança estabelecidos pelos proprietários em conformidade com as exigências de segurança;

- Os curadores são responsáveis por informar e orientar os proprietários dos recursos a respeito da efetividade dos controles aplicados e sobre a disponibilidade de outras opções de controles;
- Ao curador é submetido o desafio de encontrar exigências de segurança entre dois ou mais ativos que compartilham o mesmo recurso tecnológico.

Em alguns casos, o proprietário do ativo de informação é também o proprietário dos recursos tecnológicos onde a informação é mantida. Assim, ele é responsável tanto por estabelecer quanto por aplicar os controles nos contêiner, conforme os requisitos de segurança.

CAPÍTULO 2. INSTRUMENTOS PARA MAPEAMENTO E ACOMPANHAMENTO DE ATIVOS DE INFORMAÇÃO

Neste Capítulo, é apresentado Questionário de Mapeamento de Ativos de Informação que visa um entendimento comum e inequívoco a respeito do(s) responsável(is), do(s) contêiner(es), dos requisitos de segurança e do valor do ativo de informação. Além de subsídios para identificação de potenciais ameaças e vulnerabilidades e para a avaliação de riscos como instrumentos de acompanhamento.

2.1. Questionário para Mapeamento de Ativos de Informação

1. A que setor pertence o ativo de informação?

a) Energia;

b) Comunicações;

c) Água;

d) Finanças;

e) Transportes.

f) Outro. Especificar _____.

2. Há quanto tempo o ativo de informação está em operação?

a) Menos de 02 anos;

b) Mais de 02 e menos de 05 anos;

c) Mais de 05 e menos de 10 anos;

d) Mais de 10 anos.

3. O ativo de informação suporta processos que se identificam com:

a) Produção Industrial;

b) Fornecimento de serviços essenciais para a população;

c) Serviços de comércio;

d) Ampla rede de alcance nacional;

e) Rede de serviços de topologia local.

4. Quais áreas do negócio da organização se relacionam diretamente com o ativo de informação?

a) Sistemas de informação corporativos;

b) Todo o ciclo da informação;

c) Processos de operação;

d) Processos de gestão e suporte aos negócios;

e) Redes de comunicação;

f) Gestão de suprimentos (equipamentos e componentes) e rede de fornecedores.

5. Os processos de produção de bens e serviços que dependem diretamente do ativo de informação concentram-se em:

a) Uma ampla rede de serviços para a sociedade;

b) Serviços e atividades relacionadas com a segurança pública;

c) Serviços e atividades relacionadas com o setor financeiro;

d) Atividades relacionadas com a produção;

e) Atividades relacionadas com transportes;

f) Atividades relacionadas com o setor de energia;

g) Atividades relacionadas com o setor de água/abastecimento.

6. Qual o nível de classificação do ativo de informação?

a) Altamente estratégico para o ramo de negócio em que faz parte;

b) Altamente estratégico para a economia;

c) Altamente estratégico para a ordem social;

d) Altamente estratégico para o País;

e) Altamente estratégico para as relações internacionais;

f) Altamente estratégico no apoio à pesquisa;

g) Altamente estratégico para a defesa nacional.

7. Considerando o tempo de existência do ativo de informação, é possível classificá-lo como um alvo:

a) Com frequentes ataques;

b) Com ataques dentro de limites calculados;

c) Com perdas consideradas baixas;

d) Com perdas significativas;

e) Com estatísticas de perdas que justificam mudanças de estratégias de ação.

8. O ativo de informação está localizado em área (se necessário, escolha mais de uma alternativa):

a) Sujeita a frequentes desastres naturais;

b) Sujeita a frequentes perturbações e/ou manifestações;

c) Com grande densidade demográfica;

d) Adequada ao nível de aceitação de risco.

9. O ativo de informação está sob uma plataforma tecnológica com característica:

a) Arquitetura proprietária;

b) Arquitetura aberta;

c) Arquitetura mista (proprietária e aberta);

d) Não se aplica.

10. O ativo de informação possui:

a) Dependência de fornecedor exclusivo do mercado externo;

b) Dependência de fornecedor exclusivo do mercado interno;

c) Relativa facilidade de substituição;

d) Não há dependência de fornecedor.

11. Qual a relação entre o ativo de informação e a Infraestrutura Crítica a qual ele está ligado?

a) O ativo de informação pertence a uma Infraestrutura Crítica composta por uma rede de processos concorrentes;

b) O ativo de informação pertence a uma Infraestrutura Crítica composta por uma rede de processos independentes;

c) O ativo de informação incorpora uma matriz de atividades essenciais à operação da Infraestrutura Crítica;

d) O ativo de informação se relaciona com múltiplas Infraestruturas Críticas.

12. O ativo de informação pertence a uma Infraestrutura Crítica com transações:

a) Dentro de um mesmo Estado/Município;

b) Entre Estados/Municípios distintos;

c) Entre o Brasil e outro(s) país(es).

13. O ativo de informação está hospedado em uma infraestrutura tecnológica:

a) 100% nacional;

b) 100% internacional;

c) Parte nacional e parte internacional.

14. Quanto à governança do ativo de informação:

a) Própria;

b) Compartilhada com múltiplos parceiros nacionais;

c) Compartilhada com parceiros nacionais e internacionais;

d) Dependente de um único proprietário nacional;

e) Dependente de um único proprietário internacional.

15. Como o ativo de informação está estruturado/composto?

a) O ativo de informação está 100% informatizado;

b) O ativo de informação está parcialmente informatizado;

c) O ativo de informação consiste em dados e informações físicas (em papel ou outra forma de armazenamento).

16. O ativo de informação conta com suporte técnico:

a) Próprio;

b) Terceirizado;

c) Misto;

d) Suporte técnico inexistente ou inadequado.

17. Qual o grau de conectividade do ativo de informação com as redes de informação?

a) Está conectado diretamente à Internet;

b) Está conectado à rede interna da organização;

c) Está conectado a uma rede restrita, dentro da organização;

d) Está conectado a uma rede de terceiros;

e) Não está conectado a nenhuma rede;

f) Não se aplica.

18. O ativo de informação está sujeito a riscos cujo fato gerador é:

a) Fator humano – intencional;

b) Fator humano – não intencional;

c) Eventos naturais;

d) Falhas técnicas.

19. Qual a estimativa de retorno à normalidade caso ocorram incidentes que comprometam o ativo de informação?

a) Até 02 horas;

b) Até 10 horas;

c) Até 24 horas;

d) Até 72 horas;

e) Mais de 72 horas.

20. Se houve incidentes que comprometeram o ativo de informação nos últimos três (03) anos, qual foi o tempo médio para retorno à normalidade por meio da realização dos procedimentos de contingência?

a) Menos de 02 horas;

b) Mais de 02 e menos de 10 horas;

c) Mais de 10 e menos de 24 horas;

d) Mais de 24 e menos de 72 horas;

e) Mais de 72 horas;

f) Não foi possível restaurar.

21. Caso exista histórico, que incidentes já comprometeram o ativo de informação no passado?

a) Ataques bem sucedidos;

b) Desastres naturais;

c) Incêndios;

d) Roubos e furtos;

e) Falta de suprimentos e componentes no mercado;

f) Incidentes de toda e qualquer natureza.

22. Se houver histórico de incidentes do ativo de informação, quais os pontos que originaram a maioria dos incidentes?

a) Ataques intencionais provenientes do ambiente interno da organização;

b) Ataques intencionais provenientes do ambiente externo;

c) Ataques não intencionais provenientes do ambiente interno da organização;

d) Ataques não intencionais provenientes do ambiente externo;

e) Fenômenos naturais;

f) Não foi possível identificar.

23. Entraves legais que o ativo de informação está sujeito:

a) Permanentes e muitos;

b) Permanentes e poucos;

c) Não existentes, porém há indícios de existirem a curto ou médio prazo;

d) Não existentes.

24. Principais entraves a serem superados quanto à gestão do ativo de informação (caso necessário, marque mais de uma opção):

a) A dimensão e a complexidade das infraestruturas envolvidas;

b) A interdependência entre processos;

c) A interdependência entre setores e atividades econômicas;

d) Existência de múltiplas normas e padrões técnicos;

e) Conflito entre segurança e privacidade;

f) Questões comerciais;

g) Questões organizacionais;

h) Questões legais;

i) Questões geográficas/climáticas;

j) Questões relacionadas ao tempo para a recuperação em situações de emergência;

k) Recuperação dos serviços/atividades em situações de um ataque bem sucedido/concretizado;

l) Capacitação de RH;

m) Ampliação da segurança das redes;

n) Necessidade de cooperação técnica e científica por meio de parcerias;

o) Divisão clara de responsabilidades entre vários agentes/atores intervenientes;

p) Cobertura ampla e total do esforço de monitoramento dos riscos/ameaças associados.

25. Quais os entraves para implementar um plano de contingência e recuperação do ativo de informação?

a) Orçamentário;

b) Financeiro;

c) De ordem técnica e administrativa;

d) De ordem política;

e) Capacitação e treinamento de pessoal;

f) Legais, devido à multiplicidade de normas relacionadas a Meio Ambiente, Saúde e Segurança Pública.

26. Quais elementos estão sendo utilizados para garantir a segurança do ativo de informação?

a) Identificação de vulnerabilidades;

b) Análise de riscos;

c) Equipe técnica capacitada para possíveis desastres/incidentes;

d) Suporte técnico adequado;

e) Base tecnológica com altos níveis de segurança;

f) Plano de contingência.

27. Em situação de incidente/desastre com o ativo de informação, os danos comprometem quais setores?

a) Comércio;

b) Indústria;

c) Serviços;

d) Agronegócio.

28. Em situação de incidente/desastre com o ativo de informação, qual seria a extensão do dano?

a) Municipal;

b) Estadual;

c) Regional;

d) Nacional;

e) Internacional.

29. Um ataque bem sucedido ao ativo de informação poderá se propagar em que escala?

a) Outros setores da organização;

b) Outras Infraestruturas Críticas;

c) Sociedade;

d) O ataque não gera propagação.

30. Nível de impacto esperado em caso de comprometimento do ativo de informação:

a) Apropriação indevida de funções de suporte do ativo de informação extrínsecas à Infraestrutura Crítica;

b) Paralisação dos processos produtivos de qualquer natureza em toda a organização da Infraestrutura Crítica;

c) Paralisação/interrupção de outros setores;

d) Paralisação da rede de serviços;

e) Perturbações sociais;

f) Perturbações nos serviços à população;

g) Não há impacto significativo.

31. São realizadas inovações tecnológicas no ativo de informação?

a) Sim, programadas previamente;

b) Sim, de maneira permanente;

c) Não.

32. Quanto à regulamentação, em que situação o ativo de informação se encontra?

a) Em conformidade – padrão único nacional;

b) Em conformidade – padrão internacionalmente aceito;

c) Em conformidade parcial, devido à multiplicidade de padrões;

d) Em processo de análise de conformidade;

e) Não está conforme.

33. A auditoria e fiscalização do ativo de informação são realizadas por:

a) Órgão regulador;

b) Organizações privadas;

c) Órgão regulador e organizações privadas;

d) Não há auditoria e fiscalização.

34. O ativo de informação está subordinado/pertence :

a) Ao Nível Decisório (Alta Administração);

b) Ao Nível Estratégico;

c) Ao Nível Tático;

d) Ao Nível Operacional;

e) À Colegiados e Comitês.

35. Equipe de respostas a incidentes de redes de computadores:

a) Própria;

b) Terceirizada;

c) Não possui, mas tem parcerias (CETIR Gov, CERT.br, CAIS/RNP);

d) Não possui e não tem parcerias.

36. Quanto à capacidade de recuperação do ativo de informação e das operações:

a) Recuperação total;

b) Recuperação parcial com perdas insignificantes;

c) Recuperação parcial com perdas significativas;

d) Irrecuperável.

37. Qual a situação do sistema de comunicação de alertas relacionados ao ativo de informação?

a) Eficiente;

b) Pouco eficiente;

c) Com interessados/parceiros/clientes/fornecedores;

d) Não existe sistema de comunicação de alertas.

38. Qual a situação da estrutura técnica, administrativa e financeira prevista para a prevenção de desastres/incidentes?

a) Bem estruturada;

b) Compatível com as necessidades;

c) Em planejamento;

d) Depende de parcerias e acordos de cooperação;

e) Envolve múltiplos agentes;

f) Precária.

39. A estratégia de segurança relativa ao ativo de informação é compartilhada com outros agentes?

a) Não. Somente o usuário/proprietário é responsável pela estratégia de segurança;

b) Sim. A estratégia é compartilhada com agentes privados;

c) Sim. A estratégia é compartilhada com outros governos;

d) Sim. A estratégia é compartilhada com empresas especializadas;

e) Sim. A estratégia é compartilhada com órgãos internacionais.

40. Qual a situação da política de segurança da informação e comunicações da organização?

a) Está implantada, com responsabilidades bem definidas e existe comprometimento da alta administração;

b) Está implantada, com responsabilidades bem definidas, mas sem comprometimento da alta administração;

c) Está implantada, existe comprometimento da alta administração, mas as responsabilidades ainda não foram bem definidas;

d) Está implantada, mas ainda não há comprometimento da alta administração, nem responsabilidades devidamente definidas;

e) Não está implantada, mas está em processo de elaboração;

f) Não está implantada, e ainda não está sendo elaborada.

41. Qual o nível de interdependência do ativo de informação desta Infraestrutura Crítica com outras Infraestruturas Críticas?

a) Inexistente;

b) Baixo;

c) Médio;

d) Alto;

e) Extremamente dependente.

42. A interdependência do ativo de informação está baseada na(s) infraestrutura(s) de:

a) Sistemas de Informação;

b) Instituições;

c) Ambientes de Operação;

d) Consolidação de produtos/serviços;

e) Alta segmentação de atividades;

f) Alto nível de conexão de sistemas de informação compreendendo conexões com outros ativos de informação de empresas/provedores públicos e privados;

g) Sistemas de Informação com distintas arquiteturas, independentes de formatos proprietários;

h) Sistemas informatizados com arquiteturas distribuídas no componente de acesso, proveniente de diferentes fontes e diferentes meios.

43. Quanto às interdependências existentes ou relações de dependência entre Infraestruturas Críticas:

a) Um incidente na Infraestrutura Crítica pode ocasionar efeitos/impactos em outros setores da própria Infraestrutura Crítica?

b) Um incidente na Infraestrutura Crítica pode gerar efeitos de propagação em série afetando outras Infraestruturas Críticas que possuem/apresentam uma ou mais relação de dependência?

c) Podem provocar uma ruptura na rede/cadeias (de produtores, transformadores, fabricantes, distribuidores, etc.) de suprimentos que asseguram o provimento de produtos ou prestação de serviços essenciais à manutenção das atividades da Infraestrutura Crítica?

44. Qual a natureza da dependência entre as conexões de sistemas de informação e ativos de informação com outras Infraestruturas Críticas e seus respectivos ativos de informação, ou ainda, com uma Infraestrutura Crítica provedora de informação?

a) Relação Física: ocorre quando uma Infraestrutura Crítica está dependente de outra no fornecimento e na distribuição de insumos/matérias, expressos em bens e serviços;

b) Relação de controle de informação: ocorre quando uma Infraestrutura Crítica apresenta dependência de informação proveniente de outras Infraestruturas Críticas, como insumo necessário para o seu pleno funcionamento;

c) Relação geográfica: ocorre quando duas ou mais

Infraestruturas Críticas partilham espaço territorial com o máximo de proximidade. A proximidade sugere que caso uma Infraestrutura Crítica seja afetada por determinado evento que produza risco ou colapso no seu funcionamento, as demais Infraestruturas Críticas, indexadas no perímetro, podem também ser afetadas;

d) Relação de Propriedade/de Interação: ocorre quando existe uma dependência de gestão, que se caracteriza pela noção de propriedade, complementaridade entre produtos e serviços, de administração e finanças, de tal ordem que os danos que ocorrem em uma Infraestrutura Crítica pode significativamente prejudicar as atividades de outra Infraestrutura Crítica, indexada.

45. Havendo dependência, podemos afirmar que a Infraestrutura Crítica:

a) Apresenta alto grau de integração de tarefas e atividades com outros ativos de informação, com diferentes provedores e proprietários independentes;

b) Apresenta interações entre ativos de informação com sistemas de informação cada vez mais interligados e interdependentes;

c) Em situações de emergência, ou crise, aumenta o grau de risco;

d) Nos impactos produzidos pelos seus riscos, podem ultrapassar limites nacionais, ou seja, são transfronteiras;

e) Afeta, limita a capacidade quanto a autonomia técnica, operacional e administrativa de respostas em situação de emergência.

46. Os impactos no ativo de informação são limitados geograficamente à dimensão:

a) Local;

b) Estado;

c) Região;

d) Outros países.

47. A Infraestrutura Crítica apresenta/possui uma estrutura de processos de produção de tarefas e atividades diretamente dependentes da informação, de seu ciclo e cadeia de interações. Neste caso a Infraestrutura Crítica, pode ser identificada como:

a) A Infraestrutura Crítica é uma organização de natureza exclusiva de produção, distribuição e gestão da informação;

b) A Infraestrutura Crítica depende diretamente de ativos de informação próprios;

c) A Infraestrutura Crítica depende de ativos de informação de terceiros nacionais;

d) A Infraestrutura Crítica depende de ativos de informação estrangeiros.

48. Indique o percentual de capacitação da força de trabalho do órgão em segurança da informação e comunicações, seja proprietário e/ou curador do ativo de informação:

a) 1% a 25%;

b) 26% a 50%;

c) 51% a 75%;

d) 76% a 100%;

e) Inexistente.

49. Qual a situação da política de segurança física da organização?

a) Está implantada, com responsabilidades bem definidas e existe comprometimento da alta administração;

b) Está implantada, com responsabilidades bem definidas, mas sem comprometimento da alta administração;

c) Está implantada, existe comprometimento da alta administração, mas as responsabilidades ainda não foram bem definidas;

d) Está implantada, mas ainda não há comprometimento da alta administração, nem responsabilidades devidamente definidas;

e) Não está implantada, mas está em processo de elaboração;

f) Não está implantada, e ainda não está sendo elaborada.

50. Qual a situação dos processos e atividades para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação presente no ativo de informação?

50.1. Disponibilidade:

a) Eficiente e eficaz;

b) Eficiente e pouco eficaz;

c) Pouco eficiente e eficaz;

d) Pouco eficiente e pouco eficaz;

e) Inexistente.

50.2. Integridade:

a) Eficiente e eficaz;

b) Eficiente e pouco eficaz;

c) Pouco eficiente e eficaz;

d) Pouco eficiente e pouco eficaz;

e) Inexistente.

50.3. Confidencialidade:

a) Eficiente e eficaz;

b) Eficiente e pouco eficaz;

c) Pouco eficiente e eficaz;

d) Pouco eficiente e pouco eficaz;

e) Inexistente.

50.4. Autenticidade:

a) Eficiente e eficaz;

b) Eficiente e pouco eficaz;

c) Pouco eficiente e eficaz;

d) Pouco eficiente e pouco eficaz;

e) Inexistente.

Como complemento ao questionário, é apresentado no Anexo A.1 um conjunto de formulários que visam estruturar as informações coletadas e as constatações estabelecidas durante as atividades apresentadas no Capítulo 1.

Cada ativo de informação deverá possuir seu conjunto específico de informações composto pelo questionário respondido e pelos formulários preenchidos.

2.2. Identificação de Potenciais Ameaças e Vulnerabilidades

A potencial 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, configura os riscos de segurança da informação e comunicações.

A identificação das potenciais ameaças e vulnerabilidades compreende a fase de análise dos riscos e do estabelecimento de uma avaliação e priorização dos mesmos, estando esta inserida no processo Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) que tem como objetivo a manutenção dos riscos dentro de níveis aceitáveis. (DSIC, 2009)

2.2.1. Identificação de potenciais ameaças

As ameaças, considerando a caracterização de sua fonte, são classificadas como:

- Da natureza;
- Não intencionais (falhas), e;
- Humanas (intencionais).

Um **atributo de ameaça** é uma característica discreta ou propriedade distintiva de uma ameaça. As características combinadas de uma ameaça humana descrevem a determinação e a habilidade da ameaça perseguir o seu objetivo. Tal determinação e habilidade são definidas por múltiplos atributos separados. Nas ameaças da natureza, são definidas pela sua intensidade e persistência, já nas não intencionais, são consideradas as falhas humanas e de equipamentos. A intenção deste delineamento de atributos é que cada um define uma característica distinta de uma ameaça e não há nenhuma dependência inerente entre dois atributos.

Após a identificação dos atributos, estes devem ser confrontados com a ameaça analisada, até a caracterização, o mais aproximado possível, do nível da ameaça.

Ameaças da natureza

Consideram-se ameaças da natureza, aquelas cujo acontecimento independe da ação direta do homem. Inundações, deslizamentos de terra, terremotos, furacões, tempestades, transbordamento de rios, tsunamis, entre outros, são fenômenos naturais severos, fortemente influenciados pelas características da região em que ocorrem. Quando essas ocorrências se dão em locais onde vivem seres humanos, resultando em danos (materiais e humanos) e prejuízos (sócio-econômicos), são considerados desastres naturais.

Quatro atributos são considerados na sua avaliação: **magnitude**, **previsão**, **frequência** e **duração**.

- ✓ **Magnitude:** refere-se à força do fenômeno da natureza e à sua capacidade de provocar danos e prejuízos. É classificada conforme abaixo:
  - **Alta**: O evento possui força capaz de destruir dezenas de edificações e provocar a perda de dezenas de vidas humanas e danos ambientais significativos;
  - **Média**: O evento possui força capaz de destruir algumas edificações e provocar a perda de algumas vidas humanas e algum dano ambiental;
  - **Baixa**: O evento não possui força capaz de destruir edificações, tampouco provocar a perda de vidas humanas e danos ambientais significativos.

✓ **Previsão:** refere-se à sazonalidade do fenômeno, bem como à capacidade dos órgãos oficiais em preverem o seu acontecimento. É classificada conforme abaixo:

- **Alta**: O fenômeno é regular e/ou os órgãos oficiais conseguem prevê-lo com antecedência suficiente para permitir a tomada de ações preventivas ou mitigatórias;
- **Baixa**: O fenômeno é irregular e/ou os órgãos oficiais não conseguem prevê-lo com antecedência suficiente para permitir a tomada de ações preventivas ou mitigatórias.

✓ **Frequência:** refere-se ao número de vezes em que o evento acontece em determinado período. É classificada conforme abaixo:

- **Frequente**: o fenômeno ocorre um grande número de vezes no período;
- **Raro**: o fenômeno ocorre poucas vezes no período.

✓ **Duração:** refere-se ao tempo em que a ameaça persiste, causando danos e/ou prejuízos, materiais e humanos. É classificada conforme abaixo:

- **Longa**: tempo suficiente para provocar desabrigados em áreas consideradas seguras e prejuízos materiais de grande monta;
- **Rápida**: tempo insuficiente para provocar desabrigados ou prejuízos materiais de grande monta.

Ameaças não intencionais

Consideram-se Ameaças Não Intencionais, aquelas provocadas por falhas humanas ou de equipamentos, cujo acontecimento independe de dolo. Dividem-se as ameaças não intencionais em duas categorias:

- ✓ **Humanas**: podem ser provocadas por negligência, imprudência ou imperícia;
- ✓ **Tecnológicas**: podem ser provocadas por falhas em sistemas, equipamentos ou software.

Ameaças humanas

Distinguem-se duas famílias de atributos de ameaças humanas:

- ✓ **Do recurso**: são atributos que descrevem a habilidade da fonte de ameaça em atingir o seu objetivo;
- ✓ **Do compromisso**: são atributos que descrevem a determinação da fonte de ameaça.

Dentro da família de atributos do recurso, os mesmos abrangem as características de uma fonte de ameaça que quantificam as pessoas, conhecimento e acesso disponíveis a uma ameaça, para perseguir o seu objetivo. As características do recurso são indicativas da potencialidade de uma ameaça, porque recursos maiores podem permitir que uma ameaça atinja um objetivo mais facilmente e com maior rapidez.

Neste Guia, dado seu objetivo, tratar-se-á com maiores detalhes da família de atributos do compromisso. Nestes atributos são observadas as premissas da **intensidade**, da **furtividade**, e do **tempo**, e os mesmos abrangem as características de uma ameaça que quantificam a sua determinação para perseguir um objetivo. As características do compromisso são indicativas da potencialidade de uma

ameaça, porque exemplificam a sua persistência e condições existentes para realizar o seu objetivo:

- ✓ **Intensidade**: descreve a diligência, ou a determinação persistente, da ameaça, na perseguição do seu objetivo; é uma medida de quão distante uma ameaça está disposta ir e do que ameaça está disposta a arriscar, para realizar o seu objetivo. Há três níveis da intensidade:
  - **Elevada**: a ameaça é altamente determinada a perseguir o seu objetivo e está disposta a aceitar qualquer uma e todas as consequências resultantes dessa perseguição;
  - **Média**: a ameaça moderada está determinada a perseguir o seu objetivo, e está disposta a aceitar algumas consequências negativas resultantes dessa perseguição;
  - **Baixa**: A ameaça está determinada a perseguir o seu objetivo, mas não está disposta a aceitar consequências negativas.

- ✓ **Furtividade**: descreve a habilidade da ameaça em manter um nível necessário de dissimulação de suas atividades durante toda a perseguição do seu objetivo. Quanto maior o nível de furtividade, menor será a capacidade de percepção da ameaça, tal que dificulta a busca de informações e a adoção de medidas preventivas para opor-se ou impedir ataques pela fonte de ameaça. Há três níveis de furtividade:
  - **Elevado**: A ameaça é altamente capaz de manter o nível necessário de dissimulação, durante a perseguição do seu objetivo;

- **Médio**: A ameaça é moderadamente capaz de manter o nível necessário de dissimulação na perseguição do seu objetivo, mas não pode obscurecer completamente os detalhes sobre a sua organização ou operações internas;
- **Baixo**: A ameaça não é capaz de manter um nível necessário de dissimulação durante a perseguição do seu objetivo e não consegue obscurecer detalhes sobre a sua organização ou operações internas.

✓ **Tempo**: quantifica o período de tempo que uma fonte de ameaça é capaz de se dedicar ao planejamento, ao desenvolvimento, e à organização de métodos, desdobrando-se para alcançar um objetivo. Quanto mais tempo uma ameaça puder dispor para preparar e cometer um ataque, maior o potencial que a ameaça tem para impactos indesejados.

2.2.2. Identificação de vulnerabilidades

Com relação à identificação de vulnerabilidades, faz-se necessária a análise e avaliação dos controles que foram ou serão implementados, a fim de minimizar a probabilidade de uma ameaça explorar vulnerabilidade existente.

Considera-se que uma vulnerabilidade não é provável de ser explorada ou que possua baixa probabilidade de exploração, se houver um baixo nível de interesse ou potencialidade da fonte de ameaça ou, ainda, se houver controles eficazes de proteção que possam eliminar ou reduzir significativamente o impacto de um dano.

Os sistemas de proteção abrangem o uso de controles técnicos e não técnicos:

✓ **Controles técnicos**: são as salvaguardas que são incorporadas no sistema de proteção física, no

hardware ou no software dos computadores e sistemas de tecnologia da informação (por exemplo, mecanismos de controle de acesso, mecanismos de identificação e autenticação, métodos de encriptação e softwares de detecção de intrusão);

- ✓ **Controles não técnicos**: são processos gerenciais e operacionais, tais como: políticas de segurança da informação e comunicações; procedimentos operacionais; e segurança de pessoas, física e ambiental.

Os controles técnicos e não técnicos podem ser ainda classificados como:

- ✓ **Preventivos**: inibem tentativas de violação da política de segurança e incluem dispositivos como: controle de acesso reforçado, encriptação e autenticação;
- ✓ **De detecção**: advertem sobre violações ou tentativas de violações da política da segurança e incluem dispositivos como: trilhas de auditoria, métodos de detecção de intrusão e pontos de controle.

A implementação de tais controles, durante o processo de mitigação do risco, é o resultado direto da identificação das deficiências em controles atuais ou planejados durante o processo da avaliação de risco.

Deverá ser aplicada a **Tabela de Verificação de Requisitos Mínimos necessários à Segurança das Infraestruturas Críticas da Informação**, apresentada no Capítulo 3 deste Guia, a fim de se avaliar os requisitos de segurança e os controles, já implementados ou previstos, para Proteção Física, Proteção de Sistemas, Gestão de Pessoas e Gestão de Processos de forma eficiente e sistemática.

Devem ser listados os controles implementados, para se contrapor a cada ameaça elencada, assim como as recomendações necessárias ao aperfeiçoamento do sistema, reduzindo-se assim as suas vulnerabilidades.

Como apoio a este processo, os Anexos A.2, A.3 e A.4 apresentam, respectivamente: Exemplos de Ameaças Comuns, Exemplos de Vulnerabilidades e Perfis de Ameaças.

2.3. Avaliação de Riscos dos Ativos de Informação

Nesta fase, após serem identificados os riscos considerando as ameaças e as vulnerabilidades associadas aos ativos de informação, serão estimados os níveis de exposição aos riscos de modo que os mesmos sejam avaliados e priorizados.

A avaliação dos riscos determinará se as exposições identificadas são aceitáveis ou se requerem tratamento, priorizando-os de acordo com os critérios estabelecidos pelo órgão ou entidade. Esta avaliação fornecerá a entidade uma lista de riscos ordenados por prioridade (de acordo com os critérios de avaliação de riscos) e associados aos cenários de incidentes que os provocam.

A avaliação será realizada utilizando-se uma matriz de risco na qual serão relacionados os parâmetros probabilidade e impacto, ou seja, a chance da materialização do risco versus o impacto decorrente desta materialização sobre os ativos da informação.

Como forma de facilitar a avaliação de risco é sugerida a seguinte definição para probabilidade, impacto e níveis de risco:

Tabela 2.1 – Descrição das Probabilidades

Probabilidade	Descrição
Muito improvável	1 a 10% de chance de acontecer
Improvável	11 a 30% de chance de acontecer
Possível	31 a 70% de chance de acontecer
Provável	71 a 90% de chance de acontecer
Freqüente	91 a 100% de chance de acontecer

Tabela 2.2 – Descrição dos Impactos

Impacto	Descrição*
Muito Baixo	Não existe impacto financeiro ou impacto significativo sobre a estratégia ou atividades operacionais.
Baixo	O impacto financeiro sobre a organização não deve ultrapassar os R$ 500.000,00 (quinhentos mil reais). Impacto baixo sobre a estratégia ou atividades operacionais.
Médio	O impacto financeiro sobre a organização é maior que R$ 500.000,00 (quinhentos mil reais) e menor que R$ 7.000.000,00 (sete milhões de reais). Impacto sobre a estratégia ou atividades operacionais da organização.
Alto	O impacto financeiro sobre a organização deve ultrapassar os R$ 7.000.000,00 (sete milhões de reais) e se limitar a 15.000.000,00 (quinze milhões de reais). Impacto significativo sobre a estratégia ou atividades operacionais da organização.
Muito Alto	O impacto financeiro sobre a organização deve ultrapassar os 15.000.000,00 (quinze milhões de reais). Evento catastrófico com grande impacto sobre a estratégia ou atividades operacionais da organização.

*Os valores apresentados são apenas uma sugestão, devendo ser adequados a realizada de cada entidade.

Tabela 2.3 – Probabilidade x Impacto

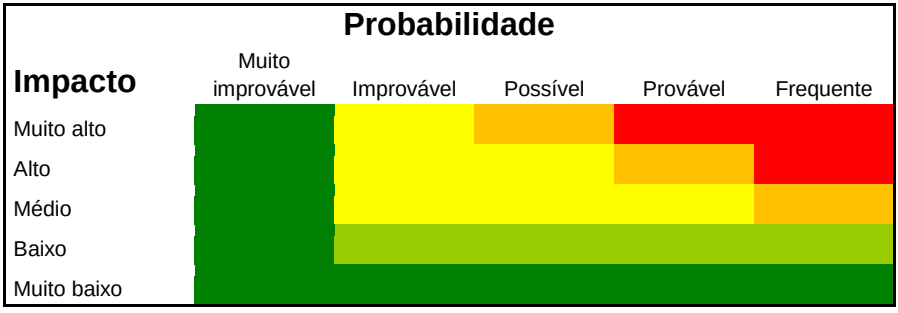


Tabela 2.4 – Descrição dos Níveis de Risco

Nível de Risco	Descrição
Muito Alto	O risco nesta faixa é intolerável. Algumas ações devem ser imediatas. Deve-se monitorar, continuamente, e observar se a situação do risco muda ao longo do tempo ou se permanece. O monitoramento deve ser contínuo.
Alto	O risco nesta faixa é intolerável. A situação é de muita preocupação e, portanto, algumas ações devem ser tomadas rapidamente. Deve-se monitorar frequentemente para verificar se a situação muda com as ações implementadas.
Médio	O risco nesta faixa é tolerável, porém existe uma situação de atenção. Algumas ações podem ser necessárias no médio ou longo prazo. Deve-se monitorar frequentemente, para verificar se a situação do risco muda ao longo do tempo, bem como se após a implementação das ações o risco diminui.
Baixo	O risco nesta faixa é tolerável. Nenhuma ação de imediato precisa ser tomada, porém deve-se monitorar, periodicamente, para verificar se a situação do risco muda com o passar do tempo.
Muito baixo	O risco nesta faixa é tolerável.

Finalizando este Capítulo, reforça-se a importância da sistematização das atividades e processos descritos, em especial com ciclos pré-definidos de melhoria contínua, incorporando ao máximo os formulários e instrumentos aqui anexados.

CAPÍTULO 3. REQUISITOS MÍNIMOS NECESSÁRIOS À SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO: SEGURANÇA, RESILIÊNCIA E CAPACITAÇÃO

O objetivo deste Capítulo é o de identificar os requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação, assim definidas como já citado anteriormente: o subconjunto de Ativos de Informação - meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso - que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade (CDN/SE, 2009).

As Infraestruturas Críticas de Informação possuem a característica de poderem fazer parte de várias Infraestruturas Críticas com relações de interdependências horizontais. Em outras palavras, a informação gerada por determinada área prioritária de Infraestruturas Críticas pode ser insumo para outra, evidenciando alto grau de acoplamento e interdependência existente entre elas. Tal grau de acoplamento eleva a necessidade da identificação dos ativos de informação, bem como o tratamento dos riscos a eles associados, pois o impacto causado pela perda ou

indisponibilidade destes ativos pode comprometer toda a cadeia de Infraestruturas Críticas.

3.1. Estratégias para Segurança das Infraestruturas Críticas da Informação

Devido à criticidade das operações e os impactos para a sociedade e governo, as organizações que compõem os setores da Infraestrutura Crítica de um país não devem conviver com crises, nem tampouco esperar por acidentes, para então tratar as questões de segurança. Toda organização deve se preparar para o impensável, adotando estratégias efetivas para evitar, minimizar, resistir e se recuperar dos efeitos das oriundas das ameaças.

São três os fatores considerados na formulação de estratégias para atender os requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação: **segurança**, **resiliência** e **capacitação**.

3.1.1. Segurança da Informação

A segurança da informação e comunicações descreve atividades que se relacionam com a proteção da informação e dos ativos da infraestrutura de informação contra riscos de perda, mau uso, divulgação indevida ou dano. É, portanto, a adoção de controles físicos, tecnológicos e humanos personalizados, que viabilizam a redução dos riscos a níveis aceitáveis, em conformidade aos requisitos de segurança exigidos pelo negócio, conforme apresentado no Capítulo 2 deste Guia.

A gestão da segurança da informação e comunicações prevê para a Segurança de Infraestruturas Criticas da

Informação controles – políticas, princípios e processos como resultados da gestão de riscos – que devem ser utilizados para garantir a minimização dos riscos. Seu foco está no nível operacional da segurança.

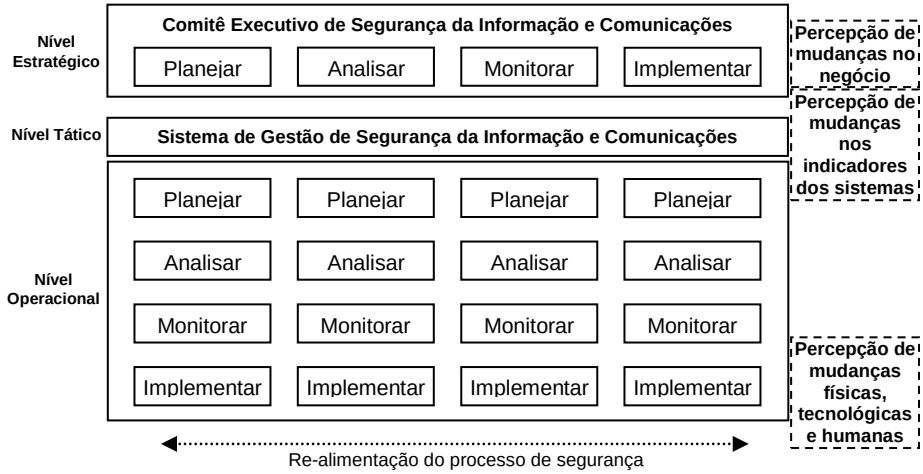


Figura 3.1 - Processo de Gestão da Segurança da Informação e Comunicações

Tendo em vista que as organizações não conseguem prever todos os desafios a serem enfrentados, é importante que sejam flexíveis e capazes de se adaptarem às mudanças no seu contexto operacional ou ambiental, de forma que possam sobreviver e principalmente evoluir. Existe a necessidade de criação e fortalecimento de uma **cultura de resiliência** entre os proprietários e operadores dos setores das Infraestruturas Críticas, com o objetivo de assegurarem que os serviços essenciais possam ser restaurados rapidamente após um desastre.

Segundo o Programa de Proteção da Infraestrutura Crítica da Austrália, existe uma preocupação no sentido de desenvolver a próxima geração de pensamento em relação à proteção das Infraestruturas Críticas, porquanto alguns estudos e pesquisas estão sendo conduzidos principalmente nos EUA, França, Nova Zelândia e na própria Austrália. Estes

países já constataram que a ações atualmente adotadas para proteção das Infraestruturas Críticas não são suficientes e já buscam orientações para uma abordagem de resiliência. O fator primordial para este direcionamento não está associado apenas à questão das ameaças, mas também a forte interdependência entre os setores das Infraestruturas Críticas, que exige uma ação coordenada, integrada e efetiva.

Considerar a resiliência sob uma perspectiva sistêmica apresenta-se com uma opção adequada para enfrentar este desafio: a proteção das Infraestruturas Críticas. A resiliência possibilita às organizações trabalharem, de forma independente e interdependente, para garantir a continuidade dos seus objetivos de negócio durante a interrupção de eventos, tais como: desastres naturais, acidentes industriais e atos terroristas, e para melhorar as parcerias com os serviços de gestão de emergência que visam assistir as comunidades.

Como abordagem inicial, a proposta é tratar a resiliência com o foco operacional considerando os segmentos de gestão da segurança da informação e comunicações, que inclui: gestão de riscos, gestão de operação de tecnologia da informação e comunicações e gestão de continuidade de negócios. Como evolução, o foco deve ser ampliado para a toda a organização, com a meta de criar uma organização resiliente.

Resiliência Operacional

De acordo com o CERT[6], engenharia de resiliência é o processo no qual uma organização projeta, desenvolve, implementa e gerencia a proteção e a sustentabilidade de seus serviços críticos, relacionados com os processos de negócio e associados aos ativos de informação. Define ainda

[6] http://www.cert.org

resiliência operacional como sendo a propriedade associada com as atividades que a organização executa visando manter serviços, processo de negócios e ativos viáveis e produtivos mesmo sob condições de risco.

Resiliência Organizacional

As organizações, como sistemas abertos, devem apresentar a capacidade de resiliência para enfrentar e superar perturbações externas provocadas pela sociedade sem que desapareça seu potencial de auto-organização. A resiliência nos negócios ganha nova urgência nos dias de hoje, influenciada por fatores como: aumento da velocidade da mudança no ambiente de negócios, pelas pressões da concorrência globalizada, um desastre natural, uma mudança econômica hostil, estratégias competitivas dos concorrentes, espionagem cibernética ou um ataque terrorista.

O *Gartner Institute*[7] diz que uma organização resiliente exige que haja um compromisso contínuo em relação ao acesso às informações, sistemas de conhecimento, mecanismos de comunicação, locais de trabalho e infraestruturas, de forma que possa rapidamente retornar à operação após um choque ou desastre.

Ser resiliente possibilita às organizações uma vantagem competitiva. Após um acidente, a organização resiliente tem maiores possibilidades de retornar à situação anterior ou à nova situação de equilíbrio de forma mais rápida, aproveitar o incidente como oportunidade para melhorar a sua eficácia, reduzir os custos com multas por não atendimento aos acordos de níveis de serviço, reduzir a exposição a perdas não previstas nos seguros, melhorar a sua reputação e aumentar a moral da equipe.

[7] http://www.gartner.com

O projeto ResOrgs[8] (*University of Canterbury – New Zealand*) estabeleceu uma metodologia para o estabelecimento de uma organização resiliente composta de 5 etapas, destacadas a seguir: criação de conscientização nas questões de resiliência; seleção de componentes organizacionais essenciais; auto avaliação das vulnerabilidades; identificação e priorização das vulnerabilidades principais; e ações visando aumentar capacidade adaptativa.

3.1.2. Capacitação (Cultura)

Nas organizações que compõem as áreas prioritárias das Infraestruturas Críticas, as ações voltadas para a cultura de segurança da informação e comunicações devem estar alinhadas e integradas com as demais ações associadas à tecnologia e processos de segurança.

Os empregados devem entender porque a segurança é importante para a sua organização e para o seu dia-a-dia. Devem saber de que forma as falhas de segurança podem afetar a organização, bem como contra o que se proteger e como se proteger.

Visando a criação e o fortalecimento da cultura de segurança da informação e comunicações, as organizações devem estabelecer ações direcionadas em três níveis: **sensibilização/conscientização**, **treinamento** e **educação**.

As ações cujos objetivos são a criação e o fortalecimento da cultura de segurança devem ser gradativas, constantes e periódicas. Estas ações precisam ser planejadas e monitoradas visando avaliar a qualidade, a efetividade e a proposição de melhorias.

[8] http://www.resorgs.org.nz/

Sensibilização e Conscientização

As ações de sensibilização e conscientização visam atingir os empregados de uma forma ampla. Buscam mudar o comportamento, reforçar boas práticas e focalizar a atenção na segurança, facilitando a implantação da Política de Segurança da Informação e Comunicações.

A sensibilização é realizada, informalmente, nas atividades cotidianas. Já a conscientização é realizada com maior formalidade, como por exemplo, por meio de palestras e seminários.

Treinamento

As ações de treinamento visam capacitar empregados que realizam funções específicas de segurança de acordo com a área de atuação. Geralmente, estes treinamentos são externos, realizado por fornecedores das soluções. Além disso, há a capacitação por meio de participação em seminários e congressos, cujos grupos de trabalho possibilitam exercitar a prática e estabelecer redes de relacionamentos técnicos.

Educação

As ações de educação visam formar especialistas, capazes de definir estratégias de segurança, servindo de apoio ao Gestor de Segurança da Informação e Comunicações da organização, ou até mesmo atuando como Gestor de Segurança setorial, dependendo da estrutura de segurança definida. As certificações em segurança devem servir como forma de manter gestores de segurança atualizados.

3.2. Requisitos mínimos necessários para a Segurança das Infraestruturas Críticas da Informação

O cerne do presente Capítulo é apresentar os requisitos para que as organizações aumentem sua segurança, resiliência e capacitação (cultura). Para isto, os controles aplicáveis aos ativos de informação são apresentados em categorias, e cada categoria é subdividida em itens de controle. Ainda, para cada item de controle, é identificado o quantitativo de detalhes necessários para que os mesmos sejam atendidos.

Tal classificação foi adaptada de artigo de YOO (2007) e está ilustrada na tabela de Verificação de Requisitos Mínimos necessários à Segurança das Infraestruturas Críticas da Informação, apresentada a seguir:

Tabela 3.1 – Tabela de Verificação de Requisitos Mínimos necessários à Segurança das Infraestruturas Críticas da Informação, adaptado de YOO (2007).

Categorias de Controle	Itens de Controle	Grau de Implementação (0 a 5 ou NA)
Política de Proteção da Informação	Organização da proteção da informação	
	Plano de proteção da informação	
	Classificação e desclassificação	
	Conformidade e entraves legais	
Gestão do Risco	Classificação de ativos	
	Alocação de recursos	
	Revisão de requisitos de segurança	
	Taxação do risco	

Categorias de Controle	Itens de Controle	Grau de Implementação (0 a 5 ou NA)
Gestão do Risco	Tratamento do risco	
	Diagnóstico de vulnerabilidades	
Gestão de Configuração	Controle de mudanças na configuração	
	Revalidação de configuração de segurança	
Manutenção	Automatização do processo	
	Manutenção remota	
	Confiabilidade (incluem contratos de níveis de serviço)	
Proteção de Mídia	Identificação da mídia de saída	
	Controle de acesso à mídia	
	Método de transporte de mídia	
	Controle da mídia	
	Armazenamento	
	Destruição / descarte de mídias e gravações	
Cultura	Treinamento	
	Conscientização	
Gestão de crise (emergência, continuidade e recuperação de desastres)	Existência dos planos (confecção, manutenção e testes)	
	Treinamento	
	Simulação e avaliação dos planos	
	Redundância de serviço	
	Backup e recuperação	

Categorias de Controle	Itens de Controle	Grau de Implementação (0 a 5 ou NA)
Proteção Física e Ambiental	Controle de acesso físico	
	Monitoramento de acesso físico	
	Proteção de instalações e linhas de energia / comunicação	
	Serviços de emergência (energia, luzes sinalizadoras, água, comunicações,...)	
	Controle de ambiente externo	
Segurança do Pessoal	Inspeção de antecedentes	
	Gestão do pessoal	
	Gestão de recursos humanos internos	
	Segurança de terceiros	
Resposta a incidentes	Treinamento simulado para incidentes	
	Monitoramento de incidentes	
	Relatório de incidentes de segurança	
	Melhoria no processo de resposta a incidentes	
Auditoria e Rastreamento de Responsabi-lidades	Definição de tópicos de auditoria	
	Gestão de informações auditadas	
	Monitoramento, análise e relatório de auditoria	
	Estabelecimento de periodicidade de auditorias	
	Penalidades administrativa, civil e penal	

Categorias de Controle	Itens de Controle	Grau de Implementação (0 a 5 ou NA)
Controle de Acesso ao Sistema e Proteção das Comunicações	Controle de contas	
	Controle de senha	
	Controle de configuração	
	Controle de acesso	
	Função de controle de falhas no acesso	
	Função destacada para precauções no uso do sistema	
	Função de relatório de informação de *login* anterior	
	Função de controle da sessão	
	Isolamento do sistema e do software aplicativo	
	Controle de recursos compartilhados do sistema	
Controle de Acesso ao Sistema e Proteção das Comunicações	Proteção contra defeitos no software e códigos maliciosos	
	Ferramentas e tecnologias para detecção de invasão e interrupção de serviço	
	Proteção contra indisponibilidade do serviço	
	Roteamento de comunicação segura	
	Criação e controle de chave criptográfica	
	Comunicação VOIP	

Categorias de Controle	Itens de Controle	Grau de Implementação (0 a 5 ou NA)
Aplicação	Segurança nas etapas do ciclo de vida dos sistemas	
	Requisitos de segurança dos sistemas	
	Processamento correto nas aplicações	
	Controles criptográficos	
	Segurança dos arquivos do sistema	
	Segurança em processos de desenvolvimento e de suporte	
	Gestão de vulnerabilidades técnicas	

Para cada item de controle deverá ser atribuído um grau de implementação que irá variar de 0 a 5, da seguinte forma: 0 a 1 = não implementado; 2 a 3 = em implementação; 4 = implementado; e 5 = otimizado. No caso de o item de controle não ser aplicável (NA), ele não computa para obtenção da média.

Após avaliar a organização quanto à média do grau de implementação de cada um dos requisitos mínimos, pode-se determinar o percentual do somatório do número de detalhes itens de controle atingidos. O resultado corresponderá ao **nível de maturidade** da organização considerada, no que diz respeito à segurança. O nível 1 corresponde a 20% de maturidade, o nível 2 a 40% e assim por diante. A descrição de tais níveis encontra-se na tabela a seguir:

Tabela 3.2 – Tabela de Nível de Maturidade de Segurança da Infraestrutura Crítica da Informação (YOO,2007).

Nível	Descrição
1	Controles de segurança não são adotados ou são executados sem um plano específico.
2	Planos de execução para os controles de segurança estão documentados e estabelecidos.
3	Controles de segurança são executados de acordo com planos documentados.
4	Controles de segurança são executados de forma consistente para um determinado período e os resultados são medidos.
5	Resultados dos controles de segurança são analisados e são adotados ajustes necessários.

É apresentado, na Tabela 3.3 que segue, o relacionamento entre os Itens de Controle, da Tabela 3.1, com o Questionário de Mapeamento de Ativos de Informação, do Capítulo 2, visando auxiliar a identificação dos níveis de maturidade a partir da ferramenta apresentada naquele Capitulo.

Tabela 3.3 – Tabela de Relacionamento de Itens de Controle X Questionário de Mapeamento de Ativos de Informação

Itens de Controle	Questionário de Mapeamento de Ativos de Informação (número da questão)
Organização da proteção da informação	#2, #10, #11, #12, #14, #25, #34, #26 e #40
Plano de proteção da informação	#39, #26 e #40
Classificação e desclassificação	#26 e #40
Conformidade e entraves legais	#32, #26 e #40
Classificação de ativos	#1, #3 e #9

Itens de Controle	Questionário de Mapeamento de Ativos de Informação (número da questão)
Alocação de recursos	#4, #5, #8 e #13
Revisão de requisitos de segurança	#6, #7 e #8
Taxação do risco	#6, #7 e #8
Tratamento do risco	#6, #40, #42, #43 e #50
Diagnóstico de vulnerabilidades	#7, #18 e #24
Controle de mudanças na configuração	#31 e #25
Revalidação de configuração de segurança	#25
Automatização do processo	#16
Manutenção remota	#16
Confiabilidade (SLA)	#16
Identificação da mídia de saída	#15
Controle de acesso à mídia	#15
Método de transporte de mídia	#15
Controle da mídia	#15
Armazenamento	#15
Destruição / descarte de mídias e gravações	#15
Treinamento	#40 e #48
Conscientização	#40 e #48
Existência dos planos (confecção, manutenção e testes)	#36
Treinamento	#36
Simulação e avaliação dos planos	#36
Redundância de serviço	#36
Backup e recuperação	#19, #20 e #36
Controle de acesso físico	#49

Itens de Controle	Questionário de Mapeamento de Ativos de Informação (número da questão)
Monitoramento de acesso físico	#49
Proteção de instalações e linhas de energia / comunicação	#49
Serviços de emergência (energia, luzes sinalizadoras, água, comunicações,...)	#49
Controle de ambiente externo	#49
Inspeção de antecedentes	#40, #48 e #49
Gestão do pessoal	#40, #48 e #49
Gestão de recursos humanos internos	#40, #48 e #49
Segurança de terceiros	#40, #48 e #49
Treinamento simulado para incidentes	#21, #22, #35, #38 e 40
Monitoramento de incidentes	#21, #22, #27, #28, #29, #35 e #38
Relatório de incidentes de segurança	#21, #22, #35 e #38
Melhoria no processo de resposta a incidentes	#21, #22, #35 e #38
Definição de tópicos de auditoria	#33
Gestão de informações auditadas	#33
Monitoramento, análise e relatório de auditoria	#33
Estabelecimento de periodicidade de auditorias	#33
Penalidades administrativa, civil e penal	#33 e #41
Controle de contas	#17 e #40
Controle de senha	#17 e #40
Controle de configuração	#17 e #40
Controle de acesso	#17 e #40

Itens de Controle	Questionário de Mapeamento de Ativos de Informação (número da questão)
Função de controle de falhas no acesso	#17, #37 e #40
Função destacada para precauções no uso do sistema	#17 e #40
Função de relatório de informação de login anterior	#17 e #40
Função de controle da sessão	#17 e #40
Isolamento do sistema e do software aplicativo	#17 e #40
Controle de recursos compartilhados do sistema	#17, #40 e # 50
Proteção contra defeitos no software e códigos maliciosos	#17, #40 e # 50
Ferramentas e tecnologias para detecção de invasão e interrupção de serviço	#17, #40 e # 50
Proteção contra indisponibilidade do serviço	#17, #40 e # 50
Roteamento de comunicação segura	#17, #40 e # 50
Criação e controle de chave criptográfica	#17, #40 e # 50
Comunicação VOIP	#17, #40 e # 50
Segurança nas etapas do ciclo de vida dos sistemas	#40 e # 50
Requisitos de segurança dos sistemas	#6, #40 e # 50
Processamento correto nas aplicações	#40 e # 50
Controles criptográficos	#6, #40 e # 50
Segurança dos arquivos do sistema	#6, #40 e # 50
Segurança em processos de desenvolvimento e de suporte	#6, #40 e # 50
Gestão de vulnerabilidades técnicas	#6, #14, #16, #17, #18, #40 e #50

O nível mínimo de maturidade de Segurança das Infraestruturas Críticas da Informação que as organizações devem se encontrar é o **nível 2**. Este nível não é a situação ideal, desta forma as organizações devem melhorar seus processos de gestão tendo como objetivo atingir o nível mais elevado de maturidade.

O Capítulo apontou diretrizes gerais para incrementar a cultura, a segurança e, num maior prazo, a resiliência das Infraestruturas Críticas da Informação.

No que diz respeito a requisitos mínimos, foi apresentada uma série de categorias e itens de controle de forma a parametrizar a situação das Infraestruturas Críticas da Informação em termos de seu nível de maturidade de segurança, considerando a identificação, o mapeamento e a gestão de ativos de informação de forma sistemática e nos níveis estratégicos, táticos e operacionais.

CAPÍTULO 4. MÉTODO DE IDENTIFICAÇÃO DE AMEAÇAS E GERAÇÃO DE ALERTAS DE SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO

Este Capítulo propõe método para identificar ameaças e para gerar alertas de Segurança das Infraestruturas Críticas da Informação, no qual se definem sensores e sinais, e se estabelecem os princípios básicos que nortearão todo método. São apresentadas as etapas que constituem o método e os modelos de articulação que poderão ser empregados, elegendo-se o modelo híbrido como mais indicado. Em seguida, é estabelecida a necessidade de uma rede de colaboração e comunicações, propondo-se sua topologia. Por fim, são expostos como será a atuação do método nas diversas Infraestruturas Críticas e aspectos que podem ser considerado como trabalhos futuros e melhorias contínuas.

4.1. Método de Identificação de Ameaças e Geração de Alertas

Com base no mapeamento de ativos de informação das Infraestruturas Críticas da Informação, apresentado nos Capítulos 1 e 2, e nos requisitos mínimos necessários à Segurança das Infraestruturas Críticas da Informação, proposto no Capítulo 3, o método trata os sinais recebidos com o objetivo de transformá-los em alertas, levando em consideração as interdependências entre as Infraestruturas Críticas, e obedecendo aos princípios de seletividade e oportunidade.

4.1.1. Sensores e Sinais

Inicialmente, para se desenvolver o método para identificação de ameaças e geração de alertas, há de se considerar a coleta de indícios de ameaças. O ideal é que tal coleta seja realizada diretamente nas Infraestruturas Críticas com base nos seus próprios controles de ativos da informação. Dessa forma, os gestores desses ativos serão responsáveis pela primeira consolidação e co-relacionamento da informação obtida.

A coleta de indícios de ameaças apresenta dois conceitos essenciais: **sensor** e **sinal**. O sensor é o elemento ou meio responsável pela coleta de informações relacionadas às ameaças, que pode pertencer tanto ao órgão gestor de ativos de informação quanto ao órgão colaborador. Sinal é a informação consolidada e inserida por um sensor na rede de identificação de ameaças e geração de alertas.

Os sinais podem variar desde informações esporádicas ou momentâneas até relatórios de situação que devem ser

remetidos em intervalos periódicos e com prazos definidos. A implantação dos controles, que deverá ser supervisionada pela coordenação setorial do órgão, irá definir o tipo de sinal que será gerado por um sensor.

4.1.2. Princípios

Os princípios gerais que devem ser seguidos pelo processo de identificação de ameaças e geração de alertas para a Segurança das Infraestruturas Críticas da Informação são a **seletividade** e a **oportunidade**.

A seletividade é definida como a faculdade de diferenciar o desejável do indesejável ou espúrio. Este princípio será empregado neste método para:

- Definir os cenários que devem ser acompanhados, levando em consideração a lista de ameaças estabelecidas;
- Estabelecer os responsáveis pelo acompanhamento de cada tipo de ameaça;
- Estabelecer um fluxo de comunicação dos sinais e de validação de ameaças; e
- Discriminar a quem devem ser direcionados os alertas, levando em consideração a necessidade de conhecer.

A oportunidade refere-se, simultaneamente, à tempestividade e à conveniência de uma ação, determinando que tal ação seja tomada de imediato e com a extensão correta. Este princípio será essencial para apoiar a concepção dos processos de forma a agilizar a comunicação das ameaças para as pessoas-chaves, garantindo que as informações inseridas no sistema alcancem os atores no tempo hábil de uma reação preventiva, e não simplesmente corretiva.

4.1.3. Etapas do método

O método para identificar ameaças e gerar alertas de Segurança das Infraestruturas Críticas da Informação, tendo sempre como fundamento os princípios da seletividade e da oportunidade, é conduzido em paralelo com a Gestão de Riscos, servindo de suporte para este, no intuito de gerar a Política de Segurança das Infraestruturas Críticas da Informação. Este método divide-se didaticamente em quatro etapas: **coleta**, **análise**, **divulgação** e **realimentação**.

Tabela 4.1 – Tabela de Etapas do Método de Identificação de Ameaças e Geração de Alertas

Etapa	Objetivos
Coleta	• Monitorar os indícios de ameaças associadas às Infraestruturas Críticas da Informação identificadas, com grau de risco predefinido, gerando sinais quando os controles indicarem um padrão de fuga da normalidade; • Acompanhar incidentes (ameaças em andamento) que afetem as Infraestruturas Críticas da Informação identificadas.
Análise	• Analisar as informações coletadas, verificando sua autenticidade; • Fazer uma triagem em termos de prioridade/impacto.
Divulgação	• Elaborar alertas com base no resultado das análises; • Divulgar os alertas, de forma segmentada, aos que necessitam conhecer, com vistas a minimizar os riscos.
Realimentação	• Validar e aperfeiçoar as técnicas de mapeamento de ativos, controle e gestão de riscos, com base nos resultados do tratamento de alertas.

4.1.4. Modelos do método

São identificados três possíveis modelos para o método:

- **Centralizado**: o órgão articulador centraliza as ameaças e emite os alertas. Esse modelo é mais vulnerável em virtude da possibilidade de se perder a oportunidade para eventual ação devido à demora e à demanda de conhecimento, processamento e estrutura. Um órgão central capaz de gerir o conhecimento de cada setor se apresenta como uma solução economicamente inviável e pouco realista, dado o vulto das Infraestruturas Críticas e a grande redundância de papéis que se insere no sistema;
- **Descentralizado**: cada setor prioritário de Infraestrutura Crítica analisa suas ameaças e emite seus alertas. Os diversos setores realizam o monitoramento e geram alertas para a rede sem qualquer análise centralizada de informações. Este modelo criaria um cenário onde a análise das interdependências não levaria em consideração o conhecimento estratégico de instâncias superiores, o que limitaria o processo de geração de alertas;
- **Híbrido**: os diversos setores adotam ações dentro de cada Infraestrutura Crítica e também possuem capacidade de gerar alertas para outros setores. O órgão articulador recebe todos os alertas, bem como aqueles sinais previamente definidos como importantes para análise estratégica e possível geração de novos alertas.

O modelo mais adequado, ora proposto, é o híbrido, pois engloba as características dos dois primeiros modelos com a vantagem de reduzir as suas limitações. Porém, é importante destacar que a seletividade da geração de alertas, especialmente no nível inter-setorial, depende da compreensão e do mapeamento das interdependências entre as diversas Infraestruturas Críticas.

4.1.5. Redes de Colaboração e Comunicação

A rede de colaboração e comunicação deve ser coordenada no âmbito nacional por um órgão articulador responsável por concentrar a evolução das ameaças e os respectivos históricos de alertas. Sugere-se que esta tarefa seja realizada pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR), dada sua competência[9]. Tal rede deverá ser composta também pelos gestores dos ativos de informação identificados e colaboradores que tenham capacidade de inserir sinais na rede.

Um segundo nível de coordenação, localizado no plano setorial, também deverá estar presente com o intuito de diminuir a necessidade de processamento do órgão articulador. A adoção de uma topologia de rede distribuída em lugar de uma centralizadora também diminui a vulnerabilidade e aumenta o grau de oportunidade do sistema.

A troca de informações nessa rede deve ser acordada via algum instrumento formal (convênio, acordo, etc.) entre os diversos atores, ou de forma coordenada. Os representantes de todas as instituições que tiverem acesso a rede devem

[9] Lei nº 10.683, de 28 de maio de 2003.

estar credenciados para tal. A Figura 4.1, a seguir, apresenta visão sobre tal rede.

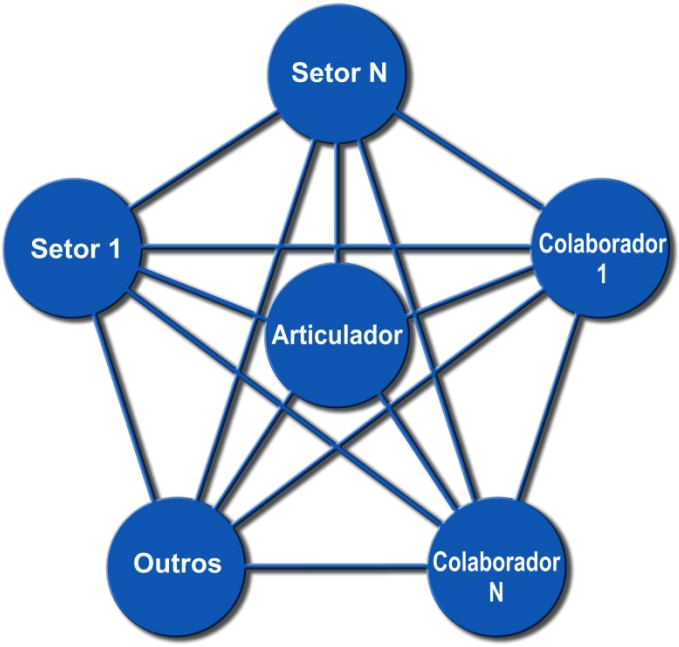


Figura 4.1 - Redes de Colaboração e Comunicação

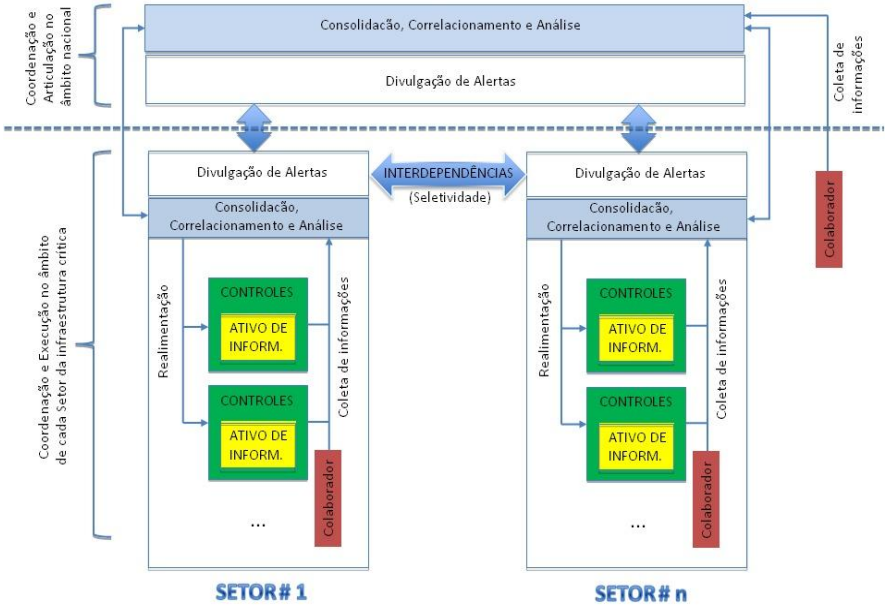
Essa rede constituirá um sistema informatizado com segurança compatível com o grau de sigilo das informações que estão nela armazenadas, com acesso segmentado às informações, conforme a necessidade de conhecer. Além disso, o sistema precisa incorporar ferramentas de análise que facilitem o tratamento de um grande volume de informações. Para atender tal demanda, pode ser adotado tanto um sistema comercial quanto um sistema desenvolvido por instituição sob gestão do órgão articulado.

4.2. Aplicação do Método

O subsistema de Infraestrutura Crítica da Informação aborda aspectos relacionados aos ativos da informação das

Infraestruturas Críticas de forma transversal, levando em consideração suas interdependências.

O método de identificação de ameaças e geração de alertas - apresentado na Figura 4.2 a seguir, denominado Módulo de Identificação de Ameaças e Geração de Alertas - compreende uma metodologia que tem como base os ativos de informação e seus respectivos controles, levando em consideração o estudo das interdependências relacionadas entre os setores.



Legenda:

Processos relacionados aos Capítulos 1 e 2

Processos relacionados ao Capítulo 3

Figura 4.2 - Módulo de Identificação de Ameaças e Geração de Alertas

Cada setor representa um segmento de Infraestrutura Crítica que pode compreender subsetores. Como exemplo, pode representar o segmento Transportes que compreende os subsetores: Aéreo, Terrestre, Aquaviário, etc. Cada subsetor é composto por organizações privadas ou públicas que seriam as responsáveis pelos ativos de informação para

os quais serão definidos controles a fim de atender requisitos mínimos de segurança da informação e comunicações. Os setores e os subsetores podem apresentar níveis distintos de maturidade de segurança que precisam ser levados em consideração para a efetividade e a confiabilidade dos alertas gerados.

Na coordenação setorial, as informações geradas pelos controles serão coletadas, consolidadas, correlacionadas e analisadas. Devem ser estabelecidos parâmetros de normalidade e as fronteiras para cada nível de alerta dentro do setor. Para cada nível de alerta, devem ser definidos planos de ações específicos.

O alerta deve ser divulgado para os setores interdependentes, bem como para a articulação do sistema de Infraestruturas Críticas da Informação. A rede de articulação do sistema de Infraestruturas Críticas da Informação também pode gerar alertas, tendo como base as informações consolidadas dos setores e informações obtidas no âmbito externo.

Com base na etapa de realimentação, os setores devem implementar ajustes em seus controles, com a finalidade de minimizar riscos em função do resultado da análise das informações coletadas.

Outros possíveis módulos visualizados para o subsistema de Infraestruturas Críticas da Informação seriam o Módulo de Gestão de Risco, Módulo de Controles Típicos (associados aos ativos de informação) e Módulo de Inventário (com o objetivo de mapear interdependências).

A proposta, portanto, de um método para identificar ameaças e gerar alertas de Segurança das Infraestruturas Críticas da Informação, apresenta como principais pontos:

- Dois conceitos essenciais para o trabalho: sensor e sinal;
- Dois princípios: seletividade e oportunidade;

- Quatro etapas: coleta, análise, divulgação e realimentação;
- Três modelos: centralizado, descentralizado e híbrido, sendo este o mais indicado;
- Uma Rede de Colaboração e Comunicação para o tráfego dos sinais;
- Um quadro com o propósito de facilitar o entendimento e a execução de ações para a identificação de ameaças e geração de alertas.

Partindo-se deste método, poderiam ser aprimorados, em termos de visão de futuro, os seguintes aspectos:

- A terminologia para identificar os elementos que fluirão pela Rede de Colaboração e Comunicação, tornando-a mais adequada e não ambígua;
- A elaboração de uma interface gráfica que mostre geograficamente as Infraestruturas Críticas da Informação monitoradas;
- A proposta de um piloto com instituições gestoras de Infraestruturas Críticas que já tenham processos implantados de monitoramento de ameaças.

CONSIDERAÇÕES FINAIS

A proposição do Guia de Referência para a Segurança das Infraestruturas Críticas da Informação é a de ponderar a respeito da importância de se despender esforços visando garantir a Segurança das Infraestruturas Críticas da Informação, dada sua criticidade para manutenção e a continuidade dos serviços essenciais prestados à sociedade e ao Estado.

Nos dias atuais, considerando as relações de interdependências que incrementam os índices de potenciais ameaças que podem assolar os ativos de informação - que compõem, ou relacionam-se com, as Infraestruturas Críticas da Informação -, deixa evidente o compromisso de se trabalhar um processo contínuo e evolutivo para o aprimoramento e refinamento do conhecimento sobre tais ativos. O efetivo conhecimento do ativo de informação é fundamental para saber do que, como e quanto pode ser investido para protegê-lo.

A proposta principal deste Guia, depreendida do seu conteúdo, é a de propor melhores práticas para Segurança das Infraestruturas Críticas da Informação e a promover uma cultura robusta sobre o tema.

Esta primeira versão do Guia apresenta os primeiros passos para sedimentar tal cultura, o que deixa patente a necessidade de ação continuada de melhorias nos métodos e instrumentos então apresentados.

É notório, portanto, que muitas ações são necessárias para criar condições preeminentes da Segurança das Infraestruturas Críticas de Informação, principalmente, no que diz respeito ao entendimento das diretrizes para a proteção da sociedade e do Estado.

GLOSSÁRIO

Alerta: é um sinal analisado e validado por um sensor na rede de identificação de ameaças e geração de alertas.

Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005).

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 (GSIPR, 2009b).

Articulador: é o órgão responsável por concentrar a evolução das ameaças e os respectivos históricos de alertas.

Ativo: qualquer coisa que tenha valor para a organização (ABNT, 2005).

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 (GSIPR, 2009d).

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 (GSIPR, 2008b).

Colaborador: é o órgão que tem capacidade de inserir sinais na rede de identificação de ameaças e geração de alertas.

Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado (GSIPR, 2008b).

Contêineres dos Ativos de Informação: o contêiner é o local onde "vive" o ativo de informação. É qualquer tipo de recurso onde a informação está armazenada, é transportada ou processada (STEVENS, 2005).

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 (GSIPR, 2009c).

Coordenação setorial: é o segundo nível de coordenação, localizado no plano setorial (vide Setor), com o intuito de diminuir a necessidade de processamento do órgão articulador e facilitar a aplicação do princípio da seletividade e oportunidade.

Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade (GSIPR, 2008b).

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 (GSIPR, 2009b).

Fonte de Risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco (ABNT, 2009a).

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 (GSIPR, 2009a).

Grau de sigilo: gradação atribuída a dado, conhecimentos, áreas ou instalações, considerados classificados, em decorrência de sua natureza ou conteúdo (adaptação do Glossário MD35-G-101, 2007).

Indícios: vestígio, indicação de algo que pode se tornar uma ameaça.

Impacto: mudança adversa no nível obtido dos objetivos do negócio (ABNT, 2008a).

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 (GSIPR, 2009d).

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 (CDN/SE, 2009).

Interdependência: relação de dependência ou interferência de uma infraestrutura crítica em outra, ou de uma área prioritária de Infraestruturas Críticas em outra (Política Nacional de Segurança de Infraestruturas Críticas, 2010 – aprovada na CREDEN, e ainda não sancionada pelo Presidente da República).

Necessidade de conhecer: condição indispensável, inerente ao exercício funcional, para que uma pessoa possuidora de credencial de segurança tenha acesso a dado e informação classificada, compatível com seu credenciamento. Desta forma a necessidade de conhecer caracteriza-se como fator restritivo de acesso, independente do grau hierárquico ou função que a pessoa exerça (adaptação do Glossário MD35-G-101, 2007).

Oportunidade: princípio que se refere, simultaneamente, à tempestividade e à conveniência de uma ação, determinando que esta seja tomada de imediato e com a extensão correta.

Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre. (NC 06 DSIC/GSIPR, 2009) Capacidade de resistir a fatores adversos e de recuperar-se rapidamente. (Política Nacional de Segurança de Infraestruturas Críticas, 2010 – aprovada na CREDEN, e ainda não sancionada pelo Presidente da República).

Risco: efeito da incerteza nos objetivos (ABNT, 2009b).

Riscos de segurança da informação: possibilidade de uma determinada ameaça explorar vulnerabilidades de um ativo ou de um conjunto de ativos, desta maneira, prejudicando a organização (ABNT, 2008b).

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. (GSIPR, 2009a).

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 infra-estruturas críticas (GSIPR, 2009d).

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 (PRESIDÊNCIA, 2000).

Segurança da Informação e Comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações (GSIPR, 2008b).

Sensor: o sensor é o elemento ou meio responsável pela coleta de informações relacionadas às ameaças.

Setor: representa um segmento de Infraestrutura Crítica que pode compreender subsetores. Como exemplo pode representar o segmento transportes que compreende os subsetores: Aéreo, Terrestre, Aquaviário, etc.

Sinal: é chamado de sinal a informação baseada em um indício ou ameaça após ser parametrizada, consolidada e inserida por um sensor na rede de identificação de ameaças e geração de alertas.

Subsetor: é um nível de especialização de um segmento de Infraestrutura Crítica, constituído por organizações privadas ou públicas responsáveis pelos ativos de informação para os quais serão definidos controles a fim de atender requisitos mínimos de segurança.

Vulnerabilidade: propriedade intrínseca de algo resultando em suscetibilidade a uma fonte de risco que pode levar a um evento com uma conseqüência (ABNT, 2009a). 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 (GSIPR, 2009a).

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. **ABNT NBR ISO/IEC 27001:2006**: Tecnologia da Informação: Técnicas de Segurança da Informação: Sistemas de Gestão de Segurança da Informação: Requisitos. Rio de Janeiro, 2006.

ABNT. **ABNT NBR ISO/IEC 27002:2005**: Tecnologia da Informação: Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ABNT. **ABNT NBR ISO/IEC 27005:2008**: Tecnologia da Informação: Técnicas de Segurança: Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008a.

ABNT. **ABNT NBR 15999-1:2007**: Gestão de Continuidade de Negócios - Parte 1: Código de prática. Rio de Janeiro, 2007

ABNT. **ABNT NBR 15999-2:2008**: Gestão de Continuidade de Negócios - Parte 2: Requisitos. Rio de Janeiro, 2008b.

ABNT. **ABNT NBR ISO 31000:2009**: Gestão de riscos - Princípios e diretrizes. Rio de Janeiro, 2009a.

ABNT. **ABNT ISO GUIA 73:2009**: Gestão de riscos - Vocabulário. Rio de Janeiro, 2009b.

BAGHERY, E. et al. **The State of the Art in Critical Infraestructure Protection: a Framework for Convergence**. Faculty of Computer Science, University of New Brunswick, Fredericton, N.B. Canada, 2007. Disponível em <http://glass.cs.unb.ca/~ebrahim/papers/CIPFramework.pdf>. Acesso em: junho, 2010.

BRUNSDON, D.; DANTAS, A. et al. **Building Organisational Resilience: A Summary of Key Research Findings**. Resilient Organisations Programme. <www.resorgs.org.nz>. Nova Zelândia, agosto de 2006.

CDN/SE. **Portaria Nº 34, de 5 de agosto de 2009**. Conselho de Defesa Nacional, Secretaria Executiva. Institui Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação - CGSI. Brasília, 2009.

CT-STI. **Ministério do Planejamento, Orçamento e Gestão, Secretaria de Logística e Tecnologia da Informação, Câmara Técnica de Segurança da Tecnologia da Informação**. Brasília, 2000. Disponível em <http://www.redegoverno.gov.br/eventos/arquivos/Mod_Seg_Inf.pdf>. Acesso em: junho, 2010.

EVERTON, G.L. et al., **Framework para Detecção e Filtragem de Alertas de Intrusão utilizando Redes Bayesianas**. Disponível em: <http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st01_03_wticg.pdf>. Acesso em: setembro, 2010.

GSIPR. **Portaria Nº 2, de 8 de fevereiro de 2008**. Gabinete de Segurança Institucional da Presidência da República. Institui Grupos Técnicos de Segurança de Infraestruturas Críticas (GTSIC) e dá outras providências. Brasília, 2008a.

GSIPR. **Instrução Normativa Nº 1, de 13 de junho de 2008.** Gabinete de Segurança Institucional da Presidência da República. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, 2008b.

GSIPR. **Norma Complementar Nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008**. Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República. Metodologia de Gestão de Segurança da Informação e Comunicações. Brasília, 2008c.

GSIPR. **Norma Complementar Nº 04/IN01/DSIC/GSIPR, de 14 de agosto de 2009**. Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República. Gestão de Riscos de Segurança da Informação e Comunicações. Brasília, 2009a.

GSIPR. **Norma Complementar Nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009**. Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República. Criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR. Brasília, 2009b.

GSIPR. **Norma Complementar Nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009**. Departamento de Segurança da Informação e Comunicações, Gabinete de Segurança Institucional da Presidência da República. Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações. Brasília, 2009c.

GSIPR. **Portaria Nº 45, de 8 de setembro de 2009**. Gabinete de Segurança Institucional da Presidência da República. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, 2009d.

LEACH, John. **"Improving User Security Behaviour"**, Computer & Security Vol 22, No 8. 2003.

LOPES, Marcos Allemand. **Conceitos da Engenharia de Resiliência Aplicados à Proteção da Infraestrutura de Informações Críticas**. Brasília, 2010.

MIN, Hyeung-Sik J.; BEYELER, Walter; BROWN, Theresa et al. Toward modeling and simulation of critical national infrastructure interdependencies. Albulquerque, 2005. Disponível em <http://www.sandia.gov/nisac/docs/IIE_HSpaper_published.pdf>. Acesso em: junho, 2010.

WILSON, Mark et al. **NIST Special Publication 800-50: Building an Information Technology Security Awareness and Training Program**. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg, 2003. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf>. Acesso em: agosto, 2010.

PRESIDÊNCIA. **Lei Nº 9.883, de 7 de dezembro de 1999**. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Brasília, 1999.

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

PRESIDÊNCIA. **Decreto Nº 4.553, de 27 de dezembro de 2002**. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Brasília, 2002.

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

SEVILLE, Erica (Dr.). **Resilience: Great Concept...But What Does it Mean for Organisations?**.Resilient Organisations, University of Canterbury. Julho de 2009.

SLTI/MPOG. **Instrução Normativa Nº 4, de 19 de maio de 2008.** Secretaria de Logística e Tecnologia da Informação, Ministério do Planejamento, Orçamento e Gestão. Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional. Brasília, 2008.

STEVENS, J. F.. **Information Asset Profiling**: CMU – Carnegie Mellon University**,** June 2005. 61 p. (CMU/SEI-2005-TN-021). Disponível em: <www.cert.org/archive/pdf/05tn021.pdf>. Acesso em: julho, 2010.

SUTER, Manuel. **A Generic National Framework for Critical Information Infrastructure (CIIP)**. Center for Security Studies, ETH. Zurique, 2007.

YOO, Dong-Young; SHIN, Jong-Whoi; LEE, Gang Shin; LEE, Jae-Il. **Improve of Evaluation Method for Information Security Levels of CIIP**. World Academy of Science, Engineering and Technology. 2007.

ANEXO A.1 FORMULÁRIOS DE APOIO PARA REGISTRO E GESTÃO DOS ATIVOS DE INFORMAÇÃO

Para auxiliar a execução do processo de Identificação e Classificação de Ativos de Informação e para ser utilizado conjunto com o Questionário de Mapeamento de Ativos de Informação, são apresentados formulários[10] que visam estruturar as informações coletadas e as constatações estabelecidas durante as atividades. Cada ativo de informação identificado deverá ter seu conjunto de formulários preenchido.

Informações Gerais do Ativo de Informação		
Data	**Versão**	**Identificação Única**
Responsáveis Preechimento (nome, cargo/função, setor, telefone/ramal, e-mail corporativo)		
Nome Ativo		**Impacto no negócio** (Alto, Médio, Baixo)
Descrição detalhada (descreva o objetivo do ativo, o que faz, como faz, requisitos utilizados, como foi desenvolvido, qual tecnologia, detalhes técnicos ...)		
Proprietário(s) do ativo (nome, cargo/função, setor, telefone/ramal, e-mail corporativo)		

[10] Adaptados de STEVENS (2005).

Contêineres do Ativo de Informação	
(1) Aplicações e Sistemas	
Aplicativos de usuários	
Sistemas Operacionais	
Sistemas Corporativos	
Outros *softwares*	
(2) Hardwares	
Servidores	
Storages	
Estações de usuários	
Outros *hardwares*	
(3) Pessoas	
Especialistas ou unidades de negócio	
Fornecedores	
Clientes	
Outras pessoas	
(4) Outros contêineres	
Locais físicos	
Papel	
Mídias magnéticas	
Outros	

Requisitos de Segurança do Ativo de Informação
Requisitos de Confidencialidade
Requisitos de Integridade
Requisitos de Disponibilidade

Relacionamentos do Ativo de Informação		
Id. Ativo	**Relacionamento Interno** (Entrada ou Saída)	**Descrição** (breve descrição do tipo do relacionamento, ex: cadastros, lançamentos, relatórios, banco de dados, memorandos, atas, solicitações, etc.)
Entidades	**Relacionamento Externo** (Entrada ou Saída)	**Descrição** (breve descrição do tipo do relacionamento, ex: manutenção, atualização, desenvolvimento, uso, etc)

Valor do Ativo de Informação	
Valor Financeiro	**Justificativa**

ANEXO A.2 EXEMPLOS DE AMEAÇAS COMUNS

A tabela abaixo contém exemplos de ameaças típicas que pode ser utilizada no processo de avaliação de ameaças. Ameaças podem ser: (I) intencionais, que indica as ações intencionais direcionadas contra os ativos da informação; (A) acidentais, que indica as ações de origem humana que podem comprometer acidentalmente e os ativos da organização; ou de origem (N) natural ou ambiental, que indica incidentes que não são provocados pela ação dos seres humanos (ABNT, 2008a):

Exemplos de ameaças comuns

Tipo	Ameaça	Origem
Dano Físico	Fogo	A, I, N
	Água	A, I, N
	Poluição	A, I, N
	Acidente grave	A, I, N
	Destruição de equipamento ou mídia	A, I, N
	Poeira, corrosão ou congelamento	A, I, N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno vulcânico	N
	Fenômeno meteorológico	N
	Inundação	N
Paralisação de serviços essenciais	Falha do condicionador de ar	A, I
	Interrupção no suprimento de energia	A, I, N
	Falha do equipamento de telecomunicações	A, I
Distúrbio causado por radiação	Radiação eletromagnética	A, I, N
	Radiação térmica	A, I, N
	Pulsos eletromagnéticos	A, I, N
Comprometimento da informação	Interceptação de sinais	I
	Espionagem à distância	I

Comprometimento da informação	Escuta não autorizada	I
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A, I
	Dados de fones não confiáveis	A, I
	Alteração do *hardware*	I
	Alteração do *software*	A, I
	Determinação da localização	I
Falhas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Saturação do sistema de informação	A, I
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitam sua manutenção	A, I
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de *software* falsificadas ou ilegais	A, I
	Comprometimento dos dados	I
	Processamento ilegal dos dados	I
Comprometimento de funções	Erro durante o uso	A
	Forjamento de direitos	A, I
	Abuso de diretos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A, I, N

Fonte: ABNT, 2008a, p. 39-40.

Abaixo, seguem fontes de ameaças representadas por seres humanos, respectivas motivações e suas possíveis conseqüências:

Exemplos de ameaças causadas por seres humanos

Fontes de ameaça	Motivação	Possíveis Consequências
Hacher, *cracker*	Desafio Egocentrismo Protesto Rebeldia *Status* Dinheiro	• *Hacking*; • Engenharia social; • Negação de serviço; • Pichação de *sites*; • Invasão de sistemas, infiltrações; • Acesso não autorizado.
Criminosos digitais	Destruição de informações Acesso a dados sigilosos Divulgação ilegal de informações Ganho monetário Alterações não autorizadas de dados	• Atos virtuais fraudulentos (interceptação de dados, ataque homem-no-meio, IP *spoofing*, etc.); • Intrusão de sistemas. • Suborno por informação; • Ataques a sistemas (negação de serviço);
Terroristas	Chantagem Destruição Vingança Exploração Ganho político Cobertura da mídia	• Ataques com bombas; • Guerra de informação; • Ataques a sistemas (negação de serviço distribuído); • Invasão e dominação de sistemas; • Alteração de sistemas.
Espiões	Vantagem competitiva Espionagem econômica	• Garantir vantagem de um posicionamento defensivo; • Garantir uma vantagem política; • Exploração econômica; • Furto de informações; • Violação da privacidade das pessoas;

Espiões		• Engenharia social; • Invasão de sistemas; • Invasão de privacidade; • Acessos não autorizados em sistemas (acesso a informação restrita, de propriedade exclusiva, e/ou relativa à tecnologia).
Pessoas: mal treinadas, insatisfeitas, mal-intencionadas, negligentes, imprudentes, desonestas, demitidas.	Curiosidade Egocentrismo Informações para serviço de Inteligência Ganhos financeiros Vingança Ações não intencionais ou omissões (erro na entrada de dados, erro na programação).	• Agressão a funcionário; • Chantagem; • Busca de informação sensível; • Abuso dos recursos computacionais; • Fraudes; • Furto de ativos; • Suborno de informação; • Inclusão de dados falsos; • Corrupção de dados; • Interceptação de informação; • Desvio de informação; • Uso de programas ou códigos maliciosos; • Sabotagens; • Invasão de sistemas; • Acessos não autorizados a sistemas.

Fonte: ABNT, 2008a, p. 40-41.

ANEXO A.3 EXEMPLOS DE VULNERABILIDADES

A tabela abaixo fornece exemplos de vulnerabilidades e possíveis ameaças em diversas áreas de segurança e pode servir de auxílio durante o processo de identificação de potenciais ameaças e vulnerabilidades, explicado no Capítulo 2.

Exemplos vulnerabilidades

Tipos	Exemplos de vulnerabilidades	Exemplos de ameaças
Hardware	Manutenção insuficiente ou instalação defeituosa de mídia de armazenamento	Violação das condições de uso do sistema de informação que possibilitam sua manutenção
	Falta de uma rotina de substituição periódica	Destruição de equipamento ou mídia
	Sensibilidade à umidade, poeira ou sujeira	Poeira, corrosão, congelamento.
	Sensibilidade à radiação eletromagnética	Radiação eletromagnética
	Inexistência de um controle de mudanças de configuração	Erro durante o uso
	Sensibilidade a variações de voltagem	Interrupção do suprimento de energia
	Sensibilidade a variações de temperatura	Fenômeno meteorológico
	Armazenamento não protegido	Furto de mídia ou documentos
	Descuidado durante o descarte	Furto de mídia ou documentos
	Utilização de cópias não controladas	Furto de mídias ou documentos
Software	Inexistência de procedimentos de teste de *softwares*.	Abuso de direitos

Software	Falhas conhecidas no *software*	Abuso de diretos
	Não execução do "*logout*" ao se deixar uma estação de trabalho	Abuso de direitos
	Descarte ou reutilização de mídia de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados	Abuso de direitos
	Inexistência de uma trilha de auditoria	Abuso de direitos
	Atribuição errônea de direitos de acesso	Abuso de diretos
	Software amplamente distribuído	Comprometimento dos dados
	Utilizar programas aplicativos com um conjunto errado de dados	Comprometimento dos dados
	Interface de usuário complexa	Erro durante uso
	Inexistência de documentação	Erro durante uso
	Parâmetros Incorretos	Erro durante uso
	Datas incorretas	Erro durante uso
Rede	Inexistência de mecanismos de autenticação e identificação	Forjamento de direitos
	Tabelas de senhas desprotegidas	Forjamento de diretos
	Gerenciamento mal feito de senhas	Forjamento de direitos
	Serviços desnecessários habilitados	Processamento ilegal de dados
	Software novo ou imaturo	Defeito de *software*
	Especificações confusas o incompletas para os desenvolvedores	Defeito de *software*

Rede	Inexistência de um controle eficaz de mudança	Defeito de *software*
	Download e uso não controlado de *software*	Alteração do *software*
	Inexistência de cópias de segurança	Alteração do *software*
	Inexistência de mecanismos de proteção física no prédio, portas e janelas	Furto de mídia ou documentos
	Inexistência de relatórios de gerenciamento	Uso não autorizado de equipamento
	Inexistência de evidências que comprovem o envio ou recebimento de mensagens	Repúdio de ações
	Linhas de Comunicação desprotegidas	Escuta não autorizada
	Tráfego sensível desprotegido	Escuta não autorizada
	Junções de cabeamento mal feitas	Falha do equipamento de telecomunicação
	Ponto único de falha	Falha do equipamento de telecomunicação
	Não identificação e não autenticação do emissor ou receptor	Forjamento de diretos
	Arquitetura insegura da rede	Espionagem à distância
	Transferências de senhas em claro	Espionagem a distância
	Gerenciamento de rede inadequado, quanto à configuração de roteamentos	Saturação do sistema de informação
	Conexões de redes públicas desprotegidas	Uso não autorizado de equipamento
Recursos humanos	Ausência de recursos humanos	Indisponibilidade de recursos humanos

Recursos humanos	Procedimentos de recrutamento inadequados	Indisponibilidade de recursos humanos
	Treinamento insuficiente em segurança	Erro durante o uso
	Uso incorreto de *software* e *hardware*	Erro durante o uso
	Falta de conscientização em segurança	Erro durante o uso
	Inexistência de mecanismos de monitoramento	Processamento ilegal dos dados
	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados	Furto de mídia ou documentos
	Inexistência de políticas pra o uso correto de meios de telecomunicação e de troca de mensagens	Uso não autorizado de recurso
Local ou instalações	Uso inadequado de mecanismos de controle de acesso físico a locais sensíveis	Destruição de equipamento ou mídia
	Localização em área suscetível a inundações	Inundação
	Fornecimento de energia instável	Interrupção de suprimento de energia
	Inexistência de mecanismos de proteção física no prédio portas e janelas	Furto de equipamentos
Organização	Inexistência de um procedimento formal para o registro de remoção de usuários	Abuso de direitos
	Inexistência de processo formal para a análise crítica dos direitos de acesso	Abuso de direitos

Organização	Provisões de segurança insuficientes o inexistentes em contratos com clientes e/ou terceiros	Abuso de direitos
	Inexistência de procedimentos de monitoramento das instalações de processamento de informações	Abuso de direitos
	Inexistência de auditorias periódicas	Abuso de direitos
	Inexistência de procedimentos para a identificação e análise/avaliação de riscos	Abuso de direitos
	Inexistência de relatos de falha nos arquivos de auditoria das atividades de administradores e operações	Abuso de direitos
	Resposta inadequada do serviço de manutenção	Violação das condições de uso do sistema de informação
	Acordo de nível de serviço (SLA) inexistência ou ineficaz	Violação das condições de uso do sistema de informação
	Controle de mudanças inexistente ou ineficaz	Violação das condições de uso do sistema de informação
	Procedimento e controle de sistemas de gerenciamento de segurança inexistentes	Comprometimento dos dados
	Atribuição inadequada das responsabilidades pela segurança da informação	Repúdio de ações
	Plano de continuidade de serviços inexistente	Falha nos serviços

Organização	Política de uso de e-mail inexistente	Erro durante o uso
	Ausência de registros de auditoria (*logs*)	Erro durante o uso
	Processo disciplinar no caso de incidentes de segurança inexistente	Furto de equipamentos ou dados
	Política de uso de recursos de informática inexistente	Furto de equipamentos ou dados
	Inexistência de controle de ativos fora da organização	Furto de equipamentos ou dados
	Inexistência de procedimentos de direitos de propriedade intelectual	Uso de cópias de aplicativos falsificadas ou ilegais.

Fonte: ABNT, 2008a, p. 42-45.

ANEXO A.4 PERFIS DE AMEAÇAS

PERFIL DA AMEAÇA								
Nível da Ameaça	HUMANA (Intencional)							
	COMPROMISSO			RECURSOS				
	Intensidade	Furtividade	Tempo	Pessoal Técnico	Conhecimento		Acesso	Financiamento
					Cibernético	Cinético		
1	A	A	A	Centenas	A	A	A	S
2	A	A	A	Dez Dez	M	A	M	S
3	A	A	M	Dez Dez	A	M	M	N
4	M	A	S	Dezenas	A	M	M	S
5	A	M	S	Dezenas	M	M	M	N
6	M	M	S	Alguns	M	M	B	S
7	M	M	M	Dezenas	B	B	B	S
8	B	B	D	Alguns	B	B	B	N

PERFIL DA AMEAÇA				
Nível da Ameaça	NATUREZA			
	Magnitude	Previsão	Duração	Frequência
1	A	B	L	F
2	A	B	R	F
3	A	A	L	R
4	M	B	L	F
5	M	B	R	F
6	M	A	L	F
7	B	B	L	R
8	B	A	R	R

PERFIL DA AMEAÇA		
Nível da Ameaça	NÃO INTENCIONAL (Falhas)	
	HUMANA	TECNOLÓGICA
1		Sistema
2	Negligência	
3		Equipamento
4	Imprudência	
5		
6	Imperícia	Software
7		
8		

ANEXO B.1 PROPOSTA DO GT SICI: ESTRUTURA GENÉRICA PARA SEGURANÇA DAS INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO

A metodologia apresentada neste Anexo e que é adotada para implementar a estratégia apresentada no Capítulo 3, baseou-se no artigo "*Generic National Framework for CIIP*" de SUTER (2007), o qual apresenta uma proposta de estrutura genérica para a Segurança das Infraestruturas Críticas da Informação.

1. Os Quatro Pilares da Segurança da Informação e Comunicações

1.1. Prevenção e alerta antecipado

Prevenção e alerta antecipado são fatores indispensáveis à Segurança da Informação e Comunicações. Deve-se buscar a prevenção por intermédio:

- Do desenvolvimento de uma cultura de Segurança da Informação e Comunicações em todos os níveis; e

- Da aplicação das demais estratégias explicadas no Capítulo 3, deste Guia, em todos os setores de interesse.

Todavia, dada a complexidade e interdependência das Infraestruturas Críticas da Informação, é inviável esperar que os incidentes possam ser prevenidos de forma conjunta. O que se pode assegurar é que:

- As Infraestruturas Críticas da Informação estejam menos vulneráveis a crises;
- As interrupções de serviço(s) sejam curtas no tempo e limitadas no espaço; e
- O(s) serviço(s) seja(m) prontamente restabelecido(s) após eventuais interrupções.

1.2. Detecção

Face à rápida evolução de novas tecnologias, as vulnerabilidades descobertas devem ser reportadas numa rede de tal forma que os alertas cheguem instantaneamente aos responsáveis pelo tratamento. No nível governamental, o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR Gov (GSIPR, 2008b), subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República, tem como finalidade precípua o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal, direta e indireta. Além disso, no Capítulo 4 deste Guia é proposto método de identificação de ameaças e geração de alertas, bem como rede de colaboração para intercâmbio de informações sobre a SICI.

1.3. Reação

A reação é composta pela identificação e correção das causas de problemas. Ressalta-se que as atividades de uma unidade que coordena a Segurança das Infraestruturas Críticas da Informação complementam, mas não substituem os esforços de cada Infraestrutura Crítica identificada. A referida unidade provê aconselhamento e direcionamento em como lidar com incidentes ao invés de oferecer soluções completas. O arcabouço legal também pode auxiliar a coibir e apurar responsabilidades, já que muitos ataques têm origem além das fronteiras físicas nacionais. A análise de incidentes também faz parte da reação, e as lições aprendidas devem ser amplamente divulgadas para realimentar o processo de revisão de normas.

1.4. Gestão de crise

É fundamental que o órgão responsável pela Segurança das Infraestruturas Críticas seja encarregado pela estrutura da gestão de crise no âmbito nacional e, numa situação adversa, tenha condições de prover aconselhamento diretamente ao Presidente da República. O GSIPR coordena, pelo Gabinete de Crise, cada demanda presidencial.

Os gestores de Segurança das Infraestruturas Críticas da Informação tendem a estar preocupados com a estrutura interna de seu órgão em detrimento das interdependências com estruturas de outros órgãos. Desta forma, o órgão responsável pela Segurança das Infraestruturas Críticas da Informação, no nível nacional, deve ter as interdependências mapeadas, bem como deve implementar oficinas e exercícios para aprimoramento do plano de gestão de crise, e para que cada Gestor de Segurança das Infraestruturas Críticas tenha a consciência do papel de sua organização em termos de interdependências.

2. Parcerias essenciais

O órgão responsável pela Segurança das Infraestruturas Críticas da Informação, no âmbito nacional, deve contar com diversas competências especializadas, podendo estar dedicada exclusivamente ou sendo selecionados pelas diversas Infraestruturas Críticas em função de suas qualificações.

Para atender as tarefas relativas aos quatro pilares da Segurança da Informação e Comunicações, há que se estabelecerem diversas competências organizacionais, técnicas e analíticas. A unidade de Segurança das Infraestruturas Críticas da Informação possui três parceiros essenciais:

- Agência governamental, provendo liderança e supervisão estratégica;
- Centro de análise articulado com o Sistema Brasileiro de Inteligência - SISBIN[11];
- Centro(s) técnico(s) com experiência no trato do assunto (CTIR Gov, CERT.br, CAIS/RNP).

2.1. Liderança e Supervisão Estratégica

As lideranças devem fazer parte da Alta Administração, embora os demais integrantes do órgão de Segurança das Infraestruturas Críticas da Informação possam ser oriundos de diversas agências governamentais.

No presente momento, o Gabinete de Segurança Institucional da Presidência da República – GSIPR, por sua competência estabelecida na Lei no 10.683, de 28 de maio de 2003, dispõe do arcabouço legal e técnico para a liderança e

[11] Lei Nº 9.883, de 7 de dezembro de 1999 e Decreto Nº 4.376, de 13 de setembro de 2002.

supervisão estratégica de SICI no âmbito nacional. É importante, também, que tal liderança tenha o reconhecimento e a confiança do setor privado.

2.2. Capacidade Analítica

Pode ser atribuída a unidades de inteligência específicas das próprias Infraestruturas Críticas que trabalham em parceria com o órgão no nível nacional. As fontes devem disponibilizar seus dados por meio de uma rede segura. É importante que o integrador das fontes trabalhe na área de inteligência para fazer a interface entre a unidade de Segurança das Infraestruturas Críticas da Informação e a inteligência. Esta função irá compor a Sala de Situação.

2.3. Competências Técnicas

O CTIR Gov deverá estar em condições de atender às demandas técnicas do órgão de Segurança das Infraestruturas Críticas da Informação do governo, e em plena sintonia com o CERT.br, o CAIS/RNP, e demais equipes de tratamento de incidentes em redes de computadores.

3. Requisitos organizacionais de uma Unidade de Segurança das Infraestruturas Críticas da Informação:

- Estrutura hierárquica enxuta: permite comunicação direta entre os integrantes.
- Responsabilidades bem definidas;

- Ter experiência em Segurança das Infraestruturas Críticas da Informação, bons contatos com decisores e com os que elaboram políticas e comunicação;
- Ter conhecimento legal e político aprofundado, bem como articulação com serviços de inteligência;
- Possuir habilidades técnicas e de comunicação.

4. Redes e ligações da Unidade de Segurança das Infraestruturas Críticas da Informação

4.1. Parcerias da chefia da unidade

- Agências governamentais envolvidas com Segurança das Infraestruturas Críticas da Informação;
- Órgãos fora da Administração Pública Federal (APF);
- Unidades estrangeiras de Segurança das Infraestruturas Críticas da Informação.

4.2. Parcerias da Sala de Situação com foco em SICI

- Casa Civil da Presidência da República;
- Gabinete de Segurança Institucional da Presidência da República;
- Agência Brasileira de Inteligência - ABIN, do Gabinete de Segurança Institucional da Presidência da República;

- Ministério da Justiça, por meio do Departamento da Polícia Federal;
- Ministério da Defesa;
- Ministério das Relações Exteriores;
- Ministério da Fazenda;
- Ministério do Trabalho e Emprego;
- Ministério da Saúde;
- Ministério da Previdência Social;
- Ministério da Ciência e Tecnologia;
- Ministério do Meio Ambiente;
- Ministério da Integração Nacional;
- Ministério do Planejamento, Orçamento e Gestão;
- INTERPOL, e outros transnacionais do gênero.

4.3. Parcerias do CTIR Gov

- CERT.br;
- CAIS/RNP;
- Demais CTIRs.

5. Clientes e Produtos

Os alvos da unidade de Segurança das Infraestruturas Críticas da Informação podem ser classificados numa base de clientes fechada (que inclui os operadores de Infraestruturas Críticas nacionais) e numa aberta (que envolvem todas as pessoas jurídicas de direito privado e computadores caseiros).

5.1. Base de Clientes Fechada

Pela própria criticidade das atividades, as Infraestruturas Críticas da Informação usualmente já possuem seus próprios especialistas para tratar de Segurança das Infraestruturas Críticas. Por isso, só é vantajoso o trato com a unidade de Segurança das Infraestruturas Críticas da Informação se esta fornecer informações relevantes para aquela Infraestrutura Crítica da Informação. Daí decorre da busca da confiança mútua.

Há que se dimensionar tal base cuidadosamente para estabelecer relacionamentos pessoais (limitando o número de representantes ou contatos de cada Infraestrutura Crítica da Informação), não superdimensionando a base. É interessante ainda separar as Infraestruturas Críticas da Informação por setores (energia, água, telecomunicações e outros).

Deve-se prover os seguintes serviços para os integrantes base de clientes:

- Assistência em caso de incidentes;
- Distribuição de informações exclusivas; e
- Oficinas, encontros e exercícios.

O benefício da partilha de informações é mútuo, particularmente em termos de experiência e conhecimento. Entretanto, cabe a cada integrante a decisão de partilhar determinadas informações consideradas críticas.

5.2. Base de Clientes Aberta

As atividades da unidade de Segurança das Infraestruturas Críticas da Informação também devem contemplar o público em geral, embora num menor grau de dedicação, posto que está bem além dos seus recursos. Tais atividades consistem nos seguintes serviços:

- Conscientização;

- Alertas e diretrizes; e
- Assistência em caso de incidentes.

O problema em lidar com tal base é a heterogeneidade dos integrantes da base e a grande expectativa que pode ser gerada por parte do público-alvo, o que pode colocar em risco a imagem da unidade de Segurança das Infraestruturas Críticas da Informação. Desta forma, há que se definir com clareza o campo de responsabilidades da unidade de Segurança das Infraestruturas Críticas da Informação perante o público.

5.3. Comparativo entre os dois modelos

Com base no que foi explanado, pode-se resumir na tabela, abaixo, as principais diferenças entre os dois modelos:

Base de Clientes	Fechada	Aberta
Membros	Operadores selecionados das Infraestruturas Críticas da Informação	Pessoas jurídicas e cidadãos
Número	2 a 4 representantes de cada membro	Indeterminado
Nível de confiança	Forte	Fraco
Construção da confiança	Contatos pessoais, reuniões e trabalho interativo	Mídia, Internet e exposições (com a ajuda dos parceiros)

ANEXO B.2 VISUALIZAÇÃO DAS CAMADAS DE SEGURANÇA

A conjugação da metodologia com os requisitos mínimos propostos no Capítulo 3 conduz ao quadro representado na Figura abaixo.

Figura: Metodologia e requisitos (LOPES, 2010)