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

Guia de Orientações ao Gestor em

Segurança da Informação e Comunicações

Versão 01 – Fev/2014

Brasília – DF
2014

Presidente da República
Dilma Roussef

Vice-Presidente da República
Michel Temer

Ministro Chefe do Gabinete de Segurança Institucional
José Elito Carvalho Siqueira

Secretário Executivo
Roberto Sebastião Peternelli Júnior

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

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

Organizadores

Danielle Rocha da Costa, Departamento de Segurança da Informação e Comunicações / GSIPR, e
José Ney de Oliveira Lima, Ministério do Planejamento, Orçamento e Gestão.

Colaboradores

Grupo de Trabalho Manual do Gestor de Segurança da Informação e Comunicações – GT MANUAL DO GESTOR DE SIC

Adelino Fernando de Souza Correia, Ministério da Saúde
Carlos de Faria Castro, Ministério da Previdência Social/INSS
Danielle Rocha da Costa, Departamento de Segurança da Informação e Comunicações / GSIPR
Eduardo Magalhães de Lacerda Filho, Instituto Nacional de Tecnologia da Informação/Casa Civil/PR
Gilson Fernando Botta, Ministério do Planejamento, Orçamento e Gestão
José Ney de Oliveira Lima, Ministério do Planejamento, Orçamento e Gestão
Juliana Rocha Munita, Ministério do Planejamento, Orçamento e Gestão
Leandro Barbosa Martins, Ministério do Planejamento, Orçamento e Gestão
Marcos Allemand Lopes, Ministério da Fazenda/SERPRO
Núbia Moreira dos Santos, Ministério do Planejamento, Orçamento e Gestão

Apoio de revisão técnica

Lucas de Oliveira Souto, Departamento de Segurança da Informação e Comunicações / GSIPR

Ficha Catalográfica
Dados Internacionais de Catalogação na Publicação (CIP)

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 Orientações ao Gestor em Segurança da Informação e Comunicações (SIC), o qual reúne métodos e instrumentos, visando orientar os gestores, com importantes aspectos inerentes à relevância 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 da Informação e Comunicações, mantendo o compromisso do Estado de promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações. Assim, motivado por esta missão, e considerando a necessidade de assegurar aos gestores uma linha de procedimentos consolidados, temos por objetivo fortalecer a cultura desta atividade de extrema necessidade no âmbito da Administração Pública Federal (APF).

Este Guia de Orientações, além de assistir a missão do GSIPR, reúne estudos técnicos sobre as legislações e normas de SIC, desenvolvidos por especialistas de diferentes órgãos e entidades da APF, direta e indireta.

O emprego da padronização e metodologia indicadas por este Guia conduzem a uma resultante avaliada e apresentada como eficiente para a organização e implementação da Segurança da Informação e Comunicações no Serviço Público. O planejamento de eventos e atividades estruturadas entrega aos gestores uma coordenação e controle de ações que minimizam vulnerabilidades organizacionais. Assim, a correta gestão do risco, baseada em sólido mapeamento de ativos de informação, assegura ao gestor dos órgãos a tranquilidade necessária ao melhor desempenho da função do órgão.

Em março de 2012 foi instituído, no âmbito do Comitê Gestor da Segurança da Informação (CGSI) um grupo de trabalho para estudo e análise de matérias relacionadas às melhores práticas e metodologias de implantação, coordenação e controle de atividades de Segurança da Informação e Comunicações. O seleto grupo foi composto por 11 servidores federais dos seguintes órgãos: GSI, MP, MS, MPS, MF e Casa Civil. Tal diversidade enriqueceu e propiciou diversas e significativas opiniões sobre o tema, as quais indubitavelmente, fomentarão discussões e propostas de melhorias sobre o assunto. Manifesto, por oportuno, minha satisfação com o resultado final obtido, fruto do esforço, dedicação e sinergia demonstrados pelo grupo de trabalho, bem como pela criteriosa apreciação do CGSI sobre o trabalho apresentado.

Recomendo, portanto, a leitura deste Guia, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Institucional, e convido-os a contribuir com propostas e sugestões para a evolução do mesmo, visando estabelecer melhores práticas de SIC no Governo Brasileiro.

Boa leitura!

José Elito Carvalho Siqueira
Ministro Chefe do Gabinete de Segurança Institucional da
Presidência da República

LISTA DE SIGLAS E ABREVIATURAS

APF	Administração Pública Federal
C3S	Central de Serviços e Suporte do SISP
CTIR GOV	Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal
DSIC	Departamento de Segurança da Informação e Comunicações
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
GCN	Gestão de Continuidade de Negócios
GRSIC	Gestão de Riscos em Segurança da Informação e Comunicações
GSI	Gabinete de Segurança Institucional
GSIC	Gestão da Segurança da Informação Comunicações
ICP – Brasil	Infraestrutura de Chaves Públicas Brasileira
INFOVIA	Infraestrutura de rede ótica metropolitana de comunicações criada para atender aos órgãos do Governo Federal
ITI	Instituto Nacional de Tecnologia da Informação
MP	Ministério do Planejamento, Orçamento e Gestão
POSIC	Política de Segurança da Informação e Comunicações
SERPRO	Serviço Federal de Processamento de Dados
SGCN	Sistema de Gestão de Continuidade de Negócios
SGSI	Sistema de Gestão de Segurança da Informação e Comunicações
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
SIC	Segurança da Informação e Comunicações
SLTI	Secretaria de Logística e Tecnologia da Informação

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

PREFÁCIO

As informações tratadas no âmbito da Administração Pública Federal, direta e indireta, são ativos valiosos para a eficiente prestação dos serviços públicos. Consequentemente, como ativo valioso e estratégico, a informação deve ser adequadamente tratada, armazenada e protegida.

Nesse contexto, o Guia de Orientações ao Gestor em Segurança da Informação e Comunicações foi elaborado com o propósito de oferecer ao leitor orientações e dicas referentes à implementação das ações de segurança da informação nas organizações públicas federais.

Cabe ressaltar que o guia toma como referência fundamental o conjunto de normas e documentos elaborados sob a coordenação do Departamento de Segurança da Informação e Comunicações (DSIC), do Gabinete de Segurança Institucional da Presidência da República (GSIPR), disponíveis no sítio: <https://dsic.planalto.gov.br/>.

O presente trabalho foi estruturado da seguinte forma:

- **Introdução:** delineia o contexto no qual o trabalho foi desenvolvido e apresenta desafios atuais relacionados à segurança da informação e comunicações;
- **Política de Segurança da Informação e Comunicações – POSIC**: aborda os principais conceitos afetos à POSIC, considerando, entre outros tópicos, a importância da sua elaboração, implementação, atualização e divulgação;
- **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR:** orienta sobre a concepção, regulamentação e gestão da ETIR, bem como, sobre o gerenciamento de incidentes de segurança em redes de computadores;
- **Gestão de Continuidade de Negócios – GCN:** considera o processo de GCN e os potenciais benefícios de sua implementação;
- **Gestão de Riscos em Segurança da Informação e Comunicações:** trata do conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos

os ativos de informação de um determinado órgão, e equilibrá-los com os custos operacionais e financeiros envolvidos; e

- **Infraestruturas Críticas da Informação:** Este tema destaca aos gestores instalações, serviços e bens, com abrangência nacional, que se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança institucional.

Esse trabalho destina-se, portanto, contribuir com os profissionais da área de segurança da informação em seu árduo, porém gratificante, desafio de dedicar à informação, como ativo valioso que é, o adequado tratamento, armazenamento e proteção.

José Ney de Oliveira Lima
Coordenador do Grupo de Trabalho
Manual do Gestor de SIC

INTRODUÇÃO

As diretrizes e metas relacionadas ao tema Segurança da Informação de Comunicações (SIC) no planejamento estratégico de cada órgão e entidade da Administração Pública Federal (APF), com o objetivo de promover e motivar a criação de uma cultura de segurança da informação, bem como implementar e manter os controles de segurança adequados devem fazer parte da agenda estratégica do Estado brasileiro.

A informação tornou-se um recurso crescente e de fundamental importância na execução das atividades do governo brasileiro. Neste sentido, a informação e o conhecimento sobre questões relativas à SIC são fatores determinantes para a eficiência da gestão dos órgãos e entidades da APF.

No atual contexto, com a utilização de um grande volume de informações, desde a prestação de serviço público ao cidadão, bem como na tomada de decisões estratégicas, as ações exercidas possuem estreito relacionamento com a segurança da informação. Problemas decorrentes da falta de Disponibilidade, Integridade, Confidencialidade e Autenticidade (DICA) em sistemas de informação levam à necessidade de desenvolver ações permanentes e gradativas de segurança na APF. Desse cenário, surgem os seguintes desafios relacionados à SIC:

- Redes Sociais;
- Computação em nuvem;
- Aumento exponencial da utilização de dispositivos móveis;
- Problemas tecnológicos;
- Aumento da demanda de informações pelos cidadãos;
- Convergência digital;
- Leis, regulamentações e normas não unificadas;

- Aumento exponencial de compartilhamento de informações;
- Redução do custo de aquisição de tecnologias de comunicação e processamento;
- Acesso a conexões de internet em banda larga;
- Fragilidade na identificação de usuário ao acesso à internet;
- Ampla disponibilidade de técnicas e ferramentas de ataque e invasão na rede e no mercado, aliado à facilidade de uso dessas ferramentas;
- Compartilhamento de informações e ferramentas de ataque e invasão entre grupos anônimos;
- Crescimento exponencial do crime virtual;
- Exaltação por práticas ilícitas com utilização de tecnologias de informação;
- Diversificação dos perfis de ameaça: concorrente, sabotador, especulador, hacker, servidores insatisfeitos e criminosos;
- Necessidade de tratar a informação como um recurso estratégico e econômico;
- Crescente valorização da informação como principal ativo de gestão do Estado;
- Crescentes transações bilaterais com suporte da tecnologia da informação e comunicações;
- Crescente dependência da gestão do Estado por recursos de tecnologia da informação e comunicações;
- Forte dependência tecnológica;
- Interdependência entre os ativos de informação;
- Aumento dos riscos associados aos ativos de informação;
- Processos de continuidade dos serviços públicos sem um grau de maturidade adequado;
- Desconhecimento das tecnologias embutidas nas arquiteturas proprietárias; e
- Alinhamento estratégico da SIC com as atribuições institucionais dos órgãos e entidades públicos.

De uma forma geral, para tratar do tema apresentado, cabe ao Gestor de SIC as seguintes atribuições:

- Promover a cultura de segurança da informação e comunicações;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
- Propor à alta administração, recursos necessários às ações de segurança da informação e comunicações;
- Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais;
- Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos da SIC no órgão;
- Manter contato direto com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), para o trato de assuntos relativos à segurança da informação e comunicações;
- Propor normas relativas à SIC ao Comitê Gestor de SIC do Órgão;
- Responder pela SIC no órgão;
- Gerenciar a aplicação de normas e políticas de proteção aos ativos e sistemas, de acordo com a legislação vigente;
- Desenvolver a análise de risco e mapeamento de vulnerabilidades;
- Elaborar o plano estratégico de Continuidade de Negócios e Recuperação de Desastres;
- Atuar junto aos usuários finais para resolução de problemas que coloquem em risco a SIC do órgão; e
- Cuidar para que sejam observadas e aplicadas no órgão, integralmente, as normas e Políticas de Segurança da Informação e Comunicações vigentes.

Considerando o panorama exposto, este guia visa prover ao Gestor conhecimentos necessários para conduzir e planejar as ações de SIC na APF. Cabe ressaltar, que no escopo da APF, as “boas práticas” são as ações de segurança da informação e comunicações descritas no arcabouço normativo desenvolvido pelo DSIC/GSIPR.

Nesta versão inicial, este Guia irá tratar dos seguintes temas:

- Política de Segurança da Informação e Comunicações (POSIC)
- Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR)
- Gestão de Continuidade de Negócios (GCN)
- Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC)
- Infraestruturas Críticas da Informação (ICI).

1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

1.1. Objetivos

Esta sessão discorre sobre os principais conceitos afetos à Política de Segurança da Informação e Comunicações (POSIC), considerando, entre outros temas, a importância da sua elaboração, implementação, atualização e divulgação.

O Decreto Nº 3.505, de 13 de junho de 2000, que instituiu a Política de Segurança da Informação nos órgãos e entidades da APF, no seu Art. 3º, estabelece como objetivos:

> *I - dotar os órgãos e as entidades da Administração Pública Federal de instrumentos jurídicos, normativos e organizacionais que os capacitem científica, tecnológica e administrativamente a assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis;*
>
> *II - eliminar a dependência externa em relação a sistemas, equipamentos, dispositivos e atividades vinculadas à segurança dos sistemas de informação;*
>
> *III - promover a capacitação de recursos humanos para o desenvolvimento de competência científico-tecnológica em segurança da informação;*
>
> *IV - estabelecer normas jurídicas necessárias à efetiva implementação da segurança da informação;*
>
> *V - promover as ações necessárias à implementação e manutenção da segurança da informação;*
>
> *VI - promover o intercâmbio científico-tecnológico entre os órgãos e as entidades da Administração Pública Federal e as instituições públicas e privadas, sobre as atividades de segurança da informação;*

VII - promover a capacitação industrial do País com vistas à sua autonomia no desenvolvimento e na fabricação de produtos que incorporem recursos criptográficos, assim como estimular o setor produtivo a participar competitivamente do mercado de bens e de serviços relacionados com a segurança da informação; e

VIII - assegurar a interoperabilidade entre os sistemas de segurança da informação.

1.2. A Política de Segurança da Informação e Comunicações (POSIC)

A POSIC é um documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta ou indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SIC.

Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação de uma organização. Assim, deve ser entendida como uma declaração formal dos órgãos e entidades da APF acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os agentes públicos e colaboradores.

Na elaboração de uma POSIC, a organização deve se preocupar não somente com aspectos técnicos, mas, também, considerar questões comportamentais e práticas do cotidiano. Afinal, as organizações enfrentam problemas de segurança que não estão necessariamente relacionados somente aos aspectos tecnológicos.

Neste contexto, uma POSIC declara o comprometimento da alta direção organizacional com a finalidade de prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão da Segurança da Informação Comunicações (GSIC). Além disso, o estabelecimento de suas diretrizes objetiva viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação no âmbito da APF, direta e indireta.

Disponibilidade

Propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

Integridade

Propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Confidencialidade

Propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

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;

1.2.1. Responsabilidades

É recomendável que na estrutura da organização exista uma área responsável pela segurança da informação, cabendo a ela a responsabilidade pela elaboração, aprovação, implantação e revisão da POSIC.

Todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente trabalham no órgão ou entidade da APF são responsáveis pela segurança da informação, pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações.

Qualquer que seja a forma de identificação, ela deve ser pessoal e intransferível, permitindo de maneira clara e indiscutível, o seu reconhecimento.

O grau de sucesso da POSIC, no entanto, está intimamente relacionado ao patrocínio da Alta Administração, que deve ser expresso formalmente, por escrito. Quanto maior o seu comprometimento, maior a probabilidade de que a política seja eficiente e eficaz para a organização.

1.2.2. Resultados Esperados

A Instrução Normativa GSI Nº 1, de 13 de junho de 2008, destaca a importância de uma POSIC, que tem como objetivo fornecer diretrizes, critérios e suporte administrativos suficientes à implementação da SIC. Seguidamente, a Norma Complementar Nº 03/IN01/DSIC/GSIPR, estabeleceu diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da POSIC nos órgãos e entidades da APF, direta e indireta. Neste sentido, a POSIC formalizada, institucionalizada e divulgada resulta na promoção de uma cultura de SIC, por intermédio de iniciativas institucionais de sensibilização, conscientização, capacitação e especialização.

1.2.3 Institucionalização da POSIC

Para a institucionalização da POSIC no órgão ou entidade da APF, são recomendadas as seguintes ações:

- Implementar a POSIC mediante aprovação formal da autoridade máxima do órgão ou entidade;
- Garantir a provisão dos recursos necessários para a implementação; e
- Promover no órgão ou entidade a cultura de segurança da informação, promovendo atividades de sensibilização, conscientização, capacitação e especialização.

A POSIC e suas atualizações devem ser divulgadas a todos os servidores, usuários, prestadores de serviço, contratados e colaboradores que habitualmente trabalham no respectivo órgão ou entidade da APF. Adicionalmente, cabe salientar, que todos os instrumentos normativos gerados a partir da POSIC, inclusive ela própria, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

1.2.3.1 Recomendações para Institucionalização da POSIC

O Quadro 1 apresenta recomendações que devem ser observadas pelo Gestor de SIC durante o desenvolvimento, implantação e manutenção de uma POSIC.

Recomendações ao Gestor de SIC
1. **Realizar planejamento, pautado nas características do órgão ou entidade da APF.** *Considerando o contexto da organização, mapear e avaliar o que deve ser protegido.* 2. **Promover a aprovação da POSIC pela alta direção.** *O patrocínio da alta direção é fundamental para o sucesso na adoção da POSIC.* 3. **Efetuar análise dos ativos de informação que devem ser protegidos.** *Analisar o que efetivamente deve ser protegido. Caso a organização já possua políticas e programas de segurança, avaliar deficiências e fatores de risco, visando seu refinamento.* 4. **Elaborar normas estabelecendo regras e proibições.** *Devem ser elaboradas normas referentes ao uso dos ativos de informação, tais como: utilização da internet, uso de dispositivos móveis, gerenciamento de acessos físicos e lógicos, utilização do e-mail, entre outros.* 5. **Obter aprovação e apoio institucional.** *No tocante à legislação vigente (leis trabalhistas, por exemplo) e à cultura organizacional, as normas e procedimentos relacionados à POSIC devem ser lidos e aprovados pelos departamentos Jurídico e de Recursos Humanos, respectivamente.*

Recomendações ao Gestor de SIC
Além disso, a POSIC deve ter o apoio e patrocínio da alta administração. **6. Investir na educação e capacitação.** *A POSIC deve ser de conhecimento de todos na organização, além de estar sempre disponível. Para isso, é fundamental iniciativas relacionadas à educação e capacitação dos envolvidos.* **7. Fazer avaliação periodicamente.** *A fim de que não fique ultrapassada ou desatualizada, a POSIC, bem como os instrumentos normativos gerados a partir dela, devem ser revistos de acordo com a periodicidade estabelecida ou tempestivamente, quando se fizer necessário.*

Tabela 1: Recomendação de 7 (sete) passos

1.3. Elementos da Política de Segurança da Informação e Comunicações

Na elaboração da POSIC recomenda-se o envolvimento de representantes dos diferentes setores do órgão ou entidade da APF como: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento. A política deve levar em consideração a natureza e finalidade do órgão ou entidade, considerando sua missão e planejamento estratégico.

Em conformidade com a Norma Complementar Nº 03/IN01/DSIC/GSIPR é recomendável que a POSIC contemple ao menos os seguintes itens:

1.3.1. Escopo

Este item deve conter a descrição do objeto e abrangência da POSIC, estabelecendo o limite das ações que serão desenvolvidas no órgão ou entidade da APF.

1.3.2. Conceitos e definições

Este item deve conter as definições de todos os conceitos utilizados na POSIC que poderiam gerar dificuldades de interpretação.

1.3.3. Referências legais e normativas

As referências legais e normativas utilizadas para a elaboração da POSIC do órgão ou entidade da APF devem ser relacionadas neste item.

1.3.4. Princípios

Neste item devem ser relacionados os princípios que regem a segurança da informação no respectivo órgão ou entidade da APF;

1.3.5. Diretrizes Gerais

Recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as normas específicas vigentes no ordenamento jurídico:

a) Tratamento da Informação;

b) Tratamento de Incidentes de Rede;

c) Gestão de Risco;

d) Gestão de Continuidade;

e) Auditoria e Conformidade;

f) Controles de Acesso;

g) Uso de e-mail; e

h) Acesso a Internet.

1.3.6. Penalidades

Este item deve identificar as consequências e penalidades para os casos de violação da POSIC e de quebra de segurança, devendo ser proposto um termo de responsabilidade.

1.3.7. Competências e Responsabilidades

Neste item é recomendável a adoção dos seguintes procedimentos:

- Definir a estrutura para a Gestão da Segurança da Informação;
- Instituir o Gestor de Segurança da Informação do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso;
- Instituir o Comitê de Segurança da Informação; e
- Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

1.3.8. Atualização

É recomendável estabelecer a periodicidade da revisão da POSIC e dos instrumentos normativos gerados a partir dela.

1.4. Normas Complementares

A POSIC deve ser clara e objetiva, de fácil leitura e entendimento. Além disso, poderá ser complementada por normas e procedimentos que a referenciem nos níveis estratégico, tático e operacional, em conformidade com a Figura 1.

Figura 1: Políticas (Estratégico), Normas (Tático) e Procedimentos (Operacional)

De acordo com a necessidade de cada órgão da APF recomenda-se a normatização dos respectivos assuntos:

a) Tratamento da Informação;

b) Gerenciamento e Tratamento de Incidentes de Segurança em Redes Computacionais;

c) Gestão de Riscos;

d) Gestão de Continuidade de Negócios;

e) Auditoria e Conformidade;

f) Controles de Acesso;

g) Uso de e-mail;

h) Dispositivos móveis;

i) Acesso a Internet;

j) Computação em nuvem; e

k) Redes Sociais.

1.5. Referências legais e normativas

- 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.
- Instrução Normativa GSIPR Nº 1, de 13 de junho de 2008.
- Norma Complementar N º 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008.
- Norma Complementar N º 03/IN01/DSIC/GSIPR, de 30 de junho de 2009.

2. EQUIPE DE TRATAMENTO E RESPOSTAS A INCIDENTES EM REDES COMPUTACIONAIS - ETIR

2.1. Objetivo

Facilitar a atuação do Gestor na concepção, regulamentação e gestão da Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais (ETIR), e no disciplinamento do gerenciamento de incidentes de segurança em redes de computadores.

Neste eixo do Guia, não é possível definir um padrão rígido que atenda de forma apropriada às características de cada organização, considerada a complexidade, missão e visão de negócio de cada uma. Contudo, é possível descrever o conjunto geral dos tópicos e assuntos que possam auxiliar o Gestor em suas ações.

2.2. Papéis e responsabilidades

2.2.1. Papéis

2.2.1.1. Gestor de Segurança da Informação e Comunicações

Responsável por coordenar a instituição, implementação e manutenção da infraestrutura necessária da ETIR e dos processos de trabalho da equipe.

2.2.1.2. Agente Responsável

Função que tem como principais competências chefiar e gerenciar a ETIR, promover integração junto ao Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV), articular junto às áreas da organização atendidas, fornecedores e prestadores de serviços de Tecnologia da Informação e Comunicações (TIC).

2.2.1.3. Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais

Grupo de pessoas com a responsabilidade de receber, analisar, classificar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, além de armazenar registros para formação de séries históricas como subsidio estatístico.

2.2.1.4. Características comuns aos componentes

Composto de pessoas com o perfil operacional e de gerenciamento de TIC, com conhecimento do contexto tecnológico, estratégia de atuação e visão de negócio da organização.

2.2.2. Responsabilidades

2.2.2.1. Criação da ETIR

Para a criação de uma ETIR, a organização deve possuir a competência formal para administração total ou parcial da infraestrutura da rede de computadores da organização. Uma vez estabelecida a competência, com o apoio e chancela da Alta Administração, deve ser publicado, alinhado com a POSIC da organização, o documento de constituição da ETIR.

Neste sentido, cumpre evidenciar os **requisitos mínimos para a instituição da ETIR**:

- Definir sua missão - propósito e estrutura das atividades desenvolvidas. A definição da missão fornecerá a linha base para as atividades a serem desenvolvidas pela Equipe;
- Público-alvo - usuários da organização e relacionamentos externos;
- Estrutura proporcional à complexidade da organização;

- Modelo de implementação;
- Nível de autonomia; e
- Serviços que serão prestados.

2.3. Gestão da ETIR

Os Gestores de SIC são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às ETIR, nos órgãos e entidades da APF, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.

Preferencialmente, a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos. Adicionalmente, a ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo CTIR GOV.

A implementação dos serviços da ETIR deve ser gradativa e de forma compatível com a maturidade da comunidade de usuários, em conformidade com a adoção do modelo e autonomia da equipe. Sugere-se que o processo de trabalho seja modelado em forma de fluxo, com rotinas e sub-rotinas claras e estabelecidas a partir de negociações com a alta administração da organização e suas áreas de negócio, fornecedores e prestadores de serviços de TIC. Este procedimento facilitará adequações futuras advindas de mudanças tecnológicas, de estrutura administrativa, entre outras, uma vez que o processo de tratamento de incidentes de redes computacionais estará mapeado.

Destaca-se a responsabilidade da ETIR em comunicar as ocorrências de incidentes de segurança em redes de computadores ao CTIR GOV, conforme procedimentos normatizados pelo DSIC/GSIPR, específicos sobre o assunto.

2.4. Ideograma da rotina de comunicação simples e tarefas básicas da Equipe

A Figura 2 representa a comunicação e as tarefas básicas de uma ETIR.

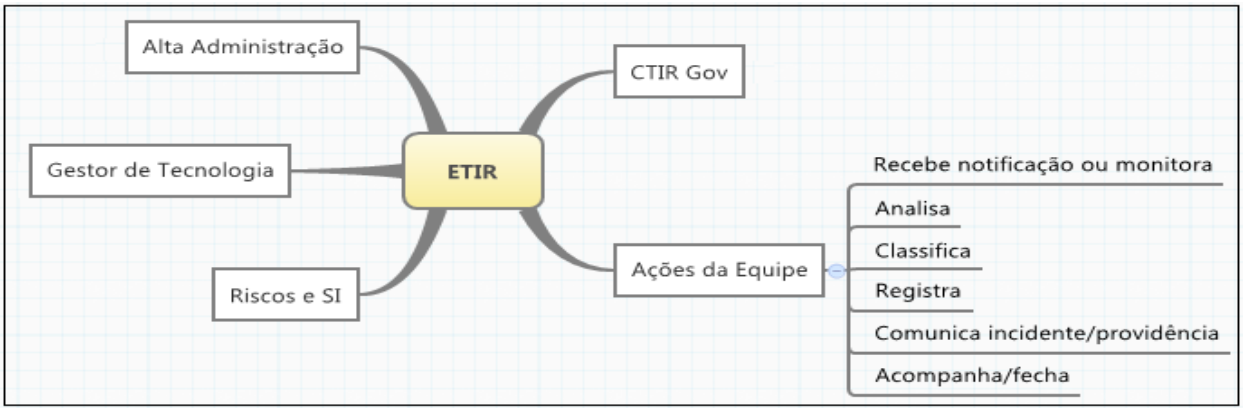

Figura 2: Todo o processo deve ser balizado pela Norma Complementar Nº 05/IN01/DSIC/GSIPR e anexo A, e Norma Complementar Nº 08/IN01/DSIC/GSIPR.

2.5. Resultados esperados

⇒ Marco institucional: ato administrativo publicado com previsão de estrutura formal mínima;

⇒ Infraestrutura de sustentação, dimensionada de acordo com o modelo, autonomia e serviços selecionados;

⇒ Classificação de incidentes;

⇒ Formulários padrão;

⇒ Processos de trabalho desenhados e atribuições definidas;

⇒ Matriz de comunicação interna e externa;

⇒ Rol de práticas e ferramentas de apoio para monitoramento dos serviços disponíveis;

⇒ Plano de capacitação continuada para a equipe; e

⇒ Composição de séries históricas como subsídio estatístico.

2.6. Etapas para alcance dos resultados

2.6.1. Cuidados no processo de criação da ETIR

A forma de atuação e autonomia da ETIR deve ajustar-se às características próprias de cada organização, suas necessidades e limitações. No momento de criação e instituição da ETIR torna-se necessário conhecer e considerar alguns fatores organizacionais como:

a) Missão institucional;

b) Porte, capilaridade e criticidade dos serviços;

c) Conhecimento do nível de maturidade e sensibilização dos servidores e/ou funcionários, parceiros de TIC em relação ao tema;

d) Nível de transferência operacional e de gestão de TI a terceiros;

e) Acordo(s) de Nível de Serviço com o(s) prestador(es) da organização; e

f) Acordos de Níveis Operacionais internos do(s) prestador(es) de serviços de TI.

2.6.2. Cuidados na definição do modelo, autonomia e serviços disponíveis

Recomendam-se 4 (quatro) modelos de implementação, 3 (três) tipos de autonomia e 9 (nove) serviços. Este cardápio de opções deve ser combinado de forma equilibrada, sempre respeitando a maturidade e as próprias restrições, pois cada órgão ou entidade deverá estabelecer, dentre os modelos apresentados abaixo, aquele que melhor se adequar às suas necessidades e limitações. Contudo, independentemente do modelo escolhido, devem ser observadas as diretrizes da Norma Complementar Nº 05/IN01/DSIC/GSIPR.

2.6.3. Opções recomendadas

2.6.3.1. Modelos

(1) Estruturado como componente da área Tecnologia da Informação - TI.

(2) Estruturado independente da área de TI, recursos operacionais e técnicos próprios.

(3) Estruturado de forma descentralizada, possui colaboradores designados nas unidades descentralizadas da organização, mas alinhados às diretrizes estabelecidas na coordenação central.

(4) Estruturado de forma combinada, é um *mix* de *2* e *3*. Ou seja, existirá uma ETIR central e suas projeções serão refletidas nas unidades descentralizadas da organização.

2.6.3.2. Autonomia

(A) **Completa** – adota decisões, iniciativas e medidas de recuperação, sem depender de níveis superiores de gestão.

(B) **Compartilhada** – compõe o processo decisório sobre medidas a serem adotadas. Recomenda procedimentos e ações. As áreas participantes do processo decisório devem ser explícitas no ato de criação da ETIR.

(C) **Sem autonomia** – age mediante a autorização de um membro da organização designado no ato de criação da ETIR.

2.6.3.3. Serviços adicionais

Além de receber, analisar, classificar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores, poderão ser oferecidos os seguintes serviços, devidamente aderentes com as normas e legislações sobre o tema:

- Tratamento de artefatos maliciosos;

- Tratamento de vulnerabilidades;
- Emissão de alertas e advertências;
- Anúncios;
- Prospecção ou monitoração de novas tecnologias;
- Avaliação de segurança;
- Desenvolvimento de ferramentas de segurança;
- Detecção de intrusão; e
- Disseminação de informações relacionadas à segurança.

2.7. Referências legais e normativas

- Instrução Normativa Nº 01 GSIPR, de 13 de junho de 2008.
- Norma Complementar Nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009 e anexo A.
- Norma Complementar Nº 08/IN01/DSIC/GSIPR, de 19 de agosto de 2010.
- Núcleo de Informação e Coordenação do Ponto BR – disponível em: <http://www.nic.br>.

3. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

3.1. Objetivo

A Gestão de Continuidade de Negócios (GCN) é um processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizam. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, e suas atividades de valor agregado.

Benefícios de um programa eficaz de GCN:

- Identificar proativamente os impactos de uma interrupção operacional;
- Ter uma resposta eficiente às interrupções, o que minimiza o impacto à organização;
- Manter a capacidade de gerenciar riscos que não podem ser segurados;
- Promover trabalho em equipe;
- Demonstrar uma resposta possível por meio de um processo de testes;
- Melhorar a reputação; e
- Obter vantagem competitiva por meio da capacidade demonstrada de manter a entrega de seus produtos e serviços.

3.2. Papéis e Responsabilidades

Os papéis e responsabilidades associados com a gestão de continuidade devem ser definidos e divulgados dentro da organização. A Tabela 2 apresenta um exemplo para estas definições, considerando uma organização de abrangência nacional e com múltiplas áreas setoriais envolvidas na gestão de continuidade.

PAPEL	RESPONSABILIDADE
Diretoria	· Assegurar a existência da gestão da continuidade para atender às necessidades da organização. · Determinar o grau de importância da gestão de continuidade. · Determinar o direcionamento estratégico. · Fornecer os recursos financeiros e humanos compatíveis com a importância e estratégia definidos. · Delegar as atividades de planejamento e coordenação do processo de gestão de continuidade ao gestor corporativo de continuidade. · Conceder ao gestor corporativo de continuidade a devida autoridade.
Coordenador corporativo de gestão de continuidade de negócios	· Coordenar o comitê corporativo de continuidade de negócios. · Posicionar a diretoria da evolução do Sistema de Gestão de Continuidade de Negócios (SGCN). · Posicionar a diretoria sobre a evolução da situação de emergência / contingência. · Planejar e coordenar a realização dos testes / exercícios corporativos.
Coordenador regional de gestão de continuidade de negócios	· Participar do comitê regional de continuidade de negócios. · Coordenar o comitê regional de continuidade de negócios. · Posicionar o Coordenador corporativo sobre a evolução das situações de emergência/contingência regionais. · Planejar e coordenar a realização dos testes / exercícios regionais.
	· Participar do comitê regional de continuidade de negócios.

PAPEL	RESPONSABILIDADE
Coordenador setorial de continuidade de negócios	· Coordenar o desenvolvimento/manutenção dos planos setoriais em conformidade com as orientações regionais. · Coordenar a elaboração/execução dos testes e exercícios regionais.
Equipe de contingência	· Elaborar/manter os planos de continuidade. · Participar dos testes e exercícios.
Comitê corporativo de continuidade de negócios	· Revisar aspectos estratégicos da GCN. · Manter o SGCN. · Apoiar o Coordenador corporativo nas situações de emergência/ desastre. · Aprovar os planos corporativos.
Comitê regional de continuidade de negócios	· Coordenar o desenvolvimento/manutenção dos planos regionais. · Aprovar os planos regionais. · Coordenar a elaboração/execução dos testes e exercícios regionais. · Coordenar as situações de emergência/desastre.

Tabela 2: Papéis e responsabilidades na gestão de continuidade de negócios.

3.3. Resultados esperados

A implantação do processo de gestão de continuidade na organização pode ser realizado por meio de um projeto específico. A Tabela 3 apresenta as etapas básicas deste projeto com os respectivos resultados esperados.

ETAPA	RESULTADOS ESPERADOS
Inicio e gestão do projeto	Apresentar a visão geral da gestão de continuidade de negócios. Apresentar as etapas principais da gestão de continuidade. Apresentar o objetivo geral do projeto. Apresentar as equipes envolvidas. Nivelar o conhecimento das equipes. Forma de trabalho definida e aprovada. Estrutura Analítica de Projeto (EAP) definida e aprovada
Entender a organização (Análise dos impactos nos negócios; Avaliação dos riscos)	Determinar a prioridade dos objetivos da organização. Determinar as funções críticas para a organização. Determinar os recursos críticos necessários para estas funções. Determinar os impactos das interrupções (financeiros, operacionais). Determinar o ponto de retomada para as operações críticas após a interrupção. Prover informação para que as estratégias apropriadas de recuperação possam ser determinadas. Requisitos de recuperação (TOR, POR MTD, WRT). Interdependências. Prioridades de recuperação dos serviços. **Análise de Risco** Explicitar os riscos para os tomadores de decisão. Se necessário, desenvolver estratégias e medidas adequadas para minimizar os riscos de forma prévia e elevar o robustez da organização. Identificar os cenários de riscos para os quais os planos de continuidade específicos devem ser desenvolvidos.

ETAPA	RESULTADOS ESPERADOS
Determinar a estratégia de continuidade	Estratégia de continuidade de cada função/sistema crítico definida, analisada sob os aspectos de viabilidade técnica e econômica, e aprovada pelo gestor do projeto (ou direção/cliente).
Desenvolver e implementar uma resposta de GCN	Política de continuidade de negócios. Papéis e responsabilidades. Organização da continuidade de negócios. Forma de acionamento dos planos. Tipos de planos de continuidade de negócios. Planos de continuidade de negócios.
Testar e manter os planos	Planos de testes capazes de validar a funcionalidade do plano de contingência. Relatório do resultado do teste contendo ajustes necessários nos planos de continuidade e no próprio plano de teste. Equipes capacitadas para conduzir as ações nas situações de contingência.
Criar e fortalecer a cultura de GCN	Estabelecer ações com o objetivo de conscientizar os empregados de uma forma geral e capacitar os empregados diretamente envolvidos com a gestão de continuidade de negócios.
Gestão do programa de GCN	Executar os processos / atividades estabelecidos por meio do SGCN.

Tabela 3: Etapas do projeto GCN – Visão geral.

3.4. Etapas para o alcance dos resultados

3.4.1. Entender a Organização – Análise de Riscos

A análise de riscos realizada no contexto da gestão de continuidade de negócios serve para identificar ameaças que possam causar a interrupção de processos de negócio e avaliar os riscos associados. Devem ser consideradas as ameaças, vulnerabilidades e impactos que possam afetar os recursos, a probabilidade dessas ocorrências, a viabilidade da adoção de controles, e a aceitação e comunicação dos riscos. Os objetivos da análise de riscos são:

- Explicitar os riscos para os tomadores de decisão.
- Se necessário, desenvolver estratégias e medidas adequadas para minimizar os riscos de forma prévia e elevar a robustez da organização.
- Identificar os cenários de riscos para os quais os planos de continuidade específicos devem ser desenvolvidos.

A abordagem típica da análise de riscos consiste na identificação das ameaças relevantes para a organização, para o processo ou para um determinado recurso, e então realizar uma avaliação dos riscos. Os seguintes aspectos devem ser considerados:

(A) É impossível identificar todos os riscos.

(B) A probabilidade de ocorrência não pode ser estimada de forma precisa.

3.4.2. Entender a organização – Análise de Impactos nos Negócios

Análise de Impacto nos Negócios (AIN): visa estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos. Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da

informação e comunicações para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos A Análise de Impactos nos Negócios, é um processo para analisar as funções de negócios e os efeitos que uma interrupção possa causar nelas.[1]

Objetivos:

- Identificar áreas de missão crítica para o negócio.
- Identificar impactos das interrupções nos negócios.
- Identificar requisitos de recuperação.
- Identificar lacunas (gaps) na capacidade de recuperação da organização.
- Estimar/justificar o orçamento do planejamento da continuidade.

Atividades a serem realizadas:

(A) Revisar conceitos e definições.

(B) Definir forma de coleta de informações.

(C) Relacionar áreas inseridas na abrangência do trabalho.

(D) Reunir com patrocinador do projeto.

(E) Workshop – início da etapa.

(F) Reunir individualmente com as áreas para analisar as informações coletadas.

(G) Análise das informações.

A AIN ajuda a entender a organização. Os impactos devem estar relacionados aos objetivos de negócio e às partes interessadas da organização:

[1] **NC nº 06/IN01/DSIC/GSIPR**, Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à SIC, nos órgãos e entidades da APF

- Estimar os impactos resultantes da interrupção de serviços e de cenários de desastres que possam afetar o desempenho dos órgãos ou entidades da APF, bem como as técnicas para quantificar e qualificar esses impactos.

- Identificar a importância das atividades da organização por meio da verificação dos impactos no tempo das interrupções e permitir o estabelecimento dos objetivos de recuperação e continuidade.

- Processo de analisar as funções de negócio e os efeitos que uma interrupção possa causar nelas.

- Processo de identificar as funções essenciais para a sobrevivência do negócio e que podem causar grande impacto se interrompidas. A análise deve considerar os impactos em uma escala de tempo.

- Estimar os impactos resultantes da interrupção de serviços e de cenários de desastre que possam afetar o desempenho da organização, bem como as técnicas para quantificar e qualificar estes impactos (ver Tabela 3). Define também a criticidade dos processos de negócio, suas prioridades de recuperação, interdependências e os requisitos de segurança da informação para que os objetivos de recuperação sejam atingidos nos prazos estabelecidos.

- Requisitos de tempos de recuperação - Tempos (janelas de tempo) importantes para a AIN nas situações de recuperação de desastres de TI (Disaster Recovery - Tabela 4 e Figura 3).

REQUISITO DE RECUPERAÇÃO	**DESCRIÇÃO**
TOR – Tempo Objetivo de Recuperação.	É o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente;
POR - Ponto objetivo de recuperação	Representa a tolerância à perda de dados como resultado de uma interrupção;

REQUISITO DE RECUPERAÇÃO	DESCRIÇÃO
TTR – Tempo de Trabalho de Recuperação	Tempo necessário para recuperar os dados perdidos ou digitar manualmente os dados coletados.
TIT - Tempo de Interrupção Tolerado	TIT = TOR + TTR

Tabela 4: Tempos a serem considerados no plano de recuperação de desastres.

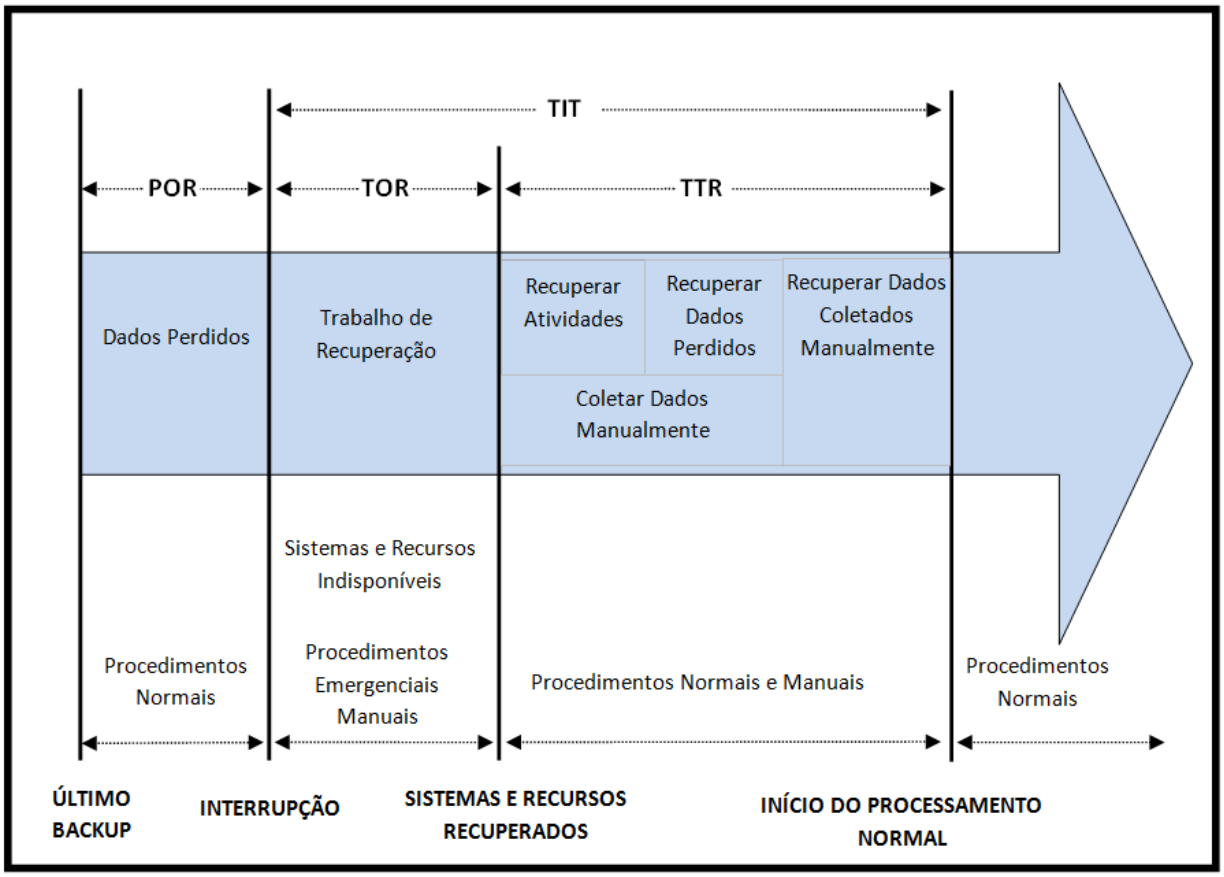

Figura 3: Tempos associados com o plano de recuperação de desastres.
Fonte: adaptação do modelo ITIL V3. .

3.4.3. Determinar a Estratégia de Continuidade

Esta etapa tem como objetivo selecionar a estratégia de continuidade apropriada ao alcance dos objetivos da organização.

A seleção de estratégias envolve:

- Objetivos da continuidade de negócios.
- Identificação de estratégias candidatas (potenciais).
- Os requisitos identificados na AIN e cenários de riscos.
- Avaliação das estratégias candidatas x AIN e Riscos.
- Consolidação das estratégias dentro da organização.
- Realizar a análise custo x benefício.
- Apresentação dos resultados/informações geradas para aprovação.

Tópicos a serem considerados:

- Uma estratégia é uma abordagem usada para uma organização tratar os riscos visando atingir os objetivos de resiliência.
- A estratégia pode dar proteção contra apenas um evento ou contra vários eventos.
- Estratégias de recuperação dão à organização capacidade para retornar às operações de forma estável após um desastre (evento).
- Durante o processo de análise, cenários de crise são úteis.
- No desenvolvimento da estratégia, o foco deve estar no que precisa ser atingido.
- A estratégia geral de recuperação deve considerar cada função/sistema crítico. As estratégias de recuperação disponíveis devem ser consideradas.
- A seleção do conjunto de estratégias depende de: custos, nível de serviço fornecido, tempo de ativação, benefícios, gerenciamento, confiança e, considerar outros planos / processos da organização.
- As estratégias devem ser selecionadas por meio da revisão e avaliação de combinações de estratégias.

- Na avaliação das estratégias, considerar a visão de longo prazo (para minimizar retrabalho e custos desnecessários).
- Quando a seleção de uma estratégia não é óbvia, deve ser realizada uma análise custo x benefício.
- Interdependências entre processos (funções / sistemas críticos).

3.4.4. Desenvolver e Implementar uma Resposta de GCN

Esta etapa tem como objetivo desenvolver e implementar uma resposta de gestão de continuidade de negócios por meio do estabelecimento das bases para o SGCN, definição de orientações para a elaboração e o próprio desenvolvimento dos planos de continuidade.

As seguintes atividades devem ser conduzidas nesta etapa do trabalho:

O primeiro ciclo requer um esforço maior, considerando a necessidade de estabelecer algumas definições básicas como a política de continuidade de negócios e a estrutura organizacional da continuidade de negócios.

Os demais ciclos devem considerar a revisão das definições já estabelecidas, quando necessário, no entanto a atividade principal estará concentrada no desenvolvimento de planos de continuidade.

- Estabelecer/rever Política de continuidade de negócios.
- Definir/revisar papéis e responsabilidades.
- Definir/revisar organização da continuidade de negócios (estrutura operacional).
- Definir/revisar forma de acionamento (processo de resposta).
- Definir /revisar forma de retorno à situação normal.
- Definir/revisar tipos de planos.
- Desenvolver/manter os planos de continuidade.

Os seguintes pontos principais devem ser considerados no desenvolvimento das atividades desta etapa:

- Escopo e objetivos para continuidade de negócios.
- Integração com outros processos da organização.
- Resultado das sistemáticas adotadas (AIN e Análise de Riscos).
- Matriz de riscos (nível aceitável de risco).
- Demais levantamentos da organização (regulamentações, missão, visão, etc.).

3.4.5. Tipos de Planos

A organização deve identificar os tipos de planos a serem adotados de acordo com o escopo definido, estratégia estabelecida e etapas do processo de resposta ao incidente. A Tabela 5 apresenta os planos definidos pela Norma Complementar Nº 06/IN01/DSIC/GSIPR – Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações elaborada pelo Departamento de Segurança da Informação e Comunicações (DSIC/GSIPR).

TIPO DE PLANO	DESCRIÇÃO
Plano de Continuidade de Negócios	Documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da APF mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes.
Plano de Gerenciamento de Incidentes	Plano de ação claramente definido e documentado, para ser usado quando ocorrer um incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes.
Plano de	Documentação dos procedimentos e informações necessárias para

Recuperação de Negócios	que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.

Tabela 5: Tipos de planos de acordo com a Norma Complementar Nº 06/IN01/DSIC/GSIPR.

3.4.6. Testar e Manter os Planos

Esta etapa tem dois objetivos principais:

- Determinar se o plano de continuidade está adequado para a recuperação dos processos de negócios dentro do período de tempo aceitável.
- Identificar lacunas e fragilidades que possam existir no plano de continuidade de negócios.

Para atingir os objetivos a etapa de testes pode envolver vários testes cada qual abordando aspectos específicos do plano geral de teste.

- Visão geral

Um plano de contingência não deve ser aprovado até ser completamente testado. O propósito da etapa de teste é portanto validar a estratégia de continuidade de negócios, suposições, atividades, procedimentos e orientações especificados no plano, considerando cenários de interrupção. A Figura 4 apresenta uma visão geral das principais etapas para o desenvolvimento de um plano de teste de plano de continuidade, destacando a fase de execução.

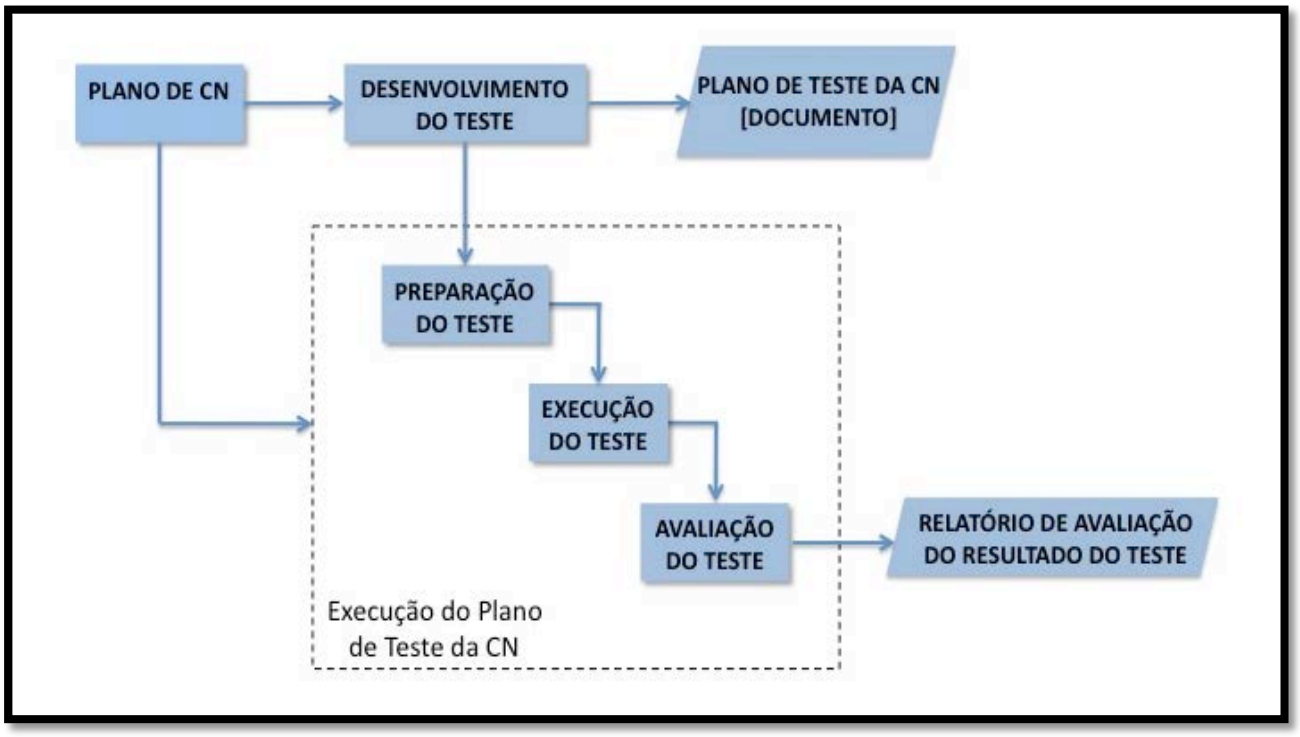

Figura 4: Etapas de execução do teste do plano de continuidade de negócios.

- Métodos de teste

A Tabela 6 apresenta os principais métodos para testar os planos de continuidade. Esses métodos variam em termos de custo, esforço e impactos na operação normal.

Checklist	É o tipo mais simples de teste e geralmente é realizado antes de testes mais complexos. De uma forma geral a equipe revisa o plano de continuidade e verifica a disponibilidade e adequação das informações e recursos necessários para a execução do plano.
Walkthrough	Geralmente denominado de teste de mesa. É um método barato. Normalmente é realizado antes de um teste de simulação. As equipes envolvidas se reúnem para descrever verbalmente suas atividades, procedimentos e atividades. Este teste permite às equipes familiarização com o plano de continuidade, recursos envolvidos e outros membros envolvidos.

Simulação	Neste teste é feita uma simulação de interrupção de acordo com cenário de desastre previamente estabelecido. Este teste permite às equipes verificarem na prática a execução do plano de continuidade e validar partes do plano.
Interrupção total	O teste de interrupção total ativa todos os componentes do plano de continuidade de negócios. Ao contrário do plano de simulação, este teste possui uma abrangência bem maior e envolve as operações e atividades reais especificadas no plano de continuidade.

Tabela 6: Principais métodos de teste para os planos de continuidade.

- Plano de Teste

Iniciar um teste de plano de contingência sem o planejamento e preparação adequados não apenas aumenta o risco de falhas como também pode causar danos à reputação das equipes e causar descrédito ao próprio processo de gestão de continuidade.

Alguns participantes consideram que os testes representam apenas perda de tempo de gastos desnecessários e, portanto, tendem a não colaborarem, principalmente quando os testes falham. Estas pessoas tendem a não participar dos testes seguintes. Da mesma forma pode ser difícil obter a aprovação dos gerentes para realizar novos testes devido aos custos e erros dos testes anteriores. Por este motivo o plano de teste deve ser cuidadosamente planejado.

O plano de teste de continuidade de negócios é um documento que fornece direcionamento para a preparação e execução do teste. Ele transmite informações críticas para as equipes envolvidas, tais como:

- Quais partes do plano de continuidade serão testadas.
- Quando e onde o teste será realizado.
- Quais recursos serão envolvidos.
- Quem vai conduzir o teste.
- Quais atividades devem ocorrer antes, durante e após o teste.
- Como o teste será avaliado.

- Quem será o observador do teste.
- O plano de teste da continuidade de negócios deve ser revisado pelas equipes para garantir os seguintes pontos:
- O plano de teste está correto, atualizado e não contém lacunas.
- O plano possui uma relação custo x benefício adequada.
- O plano é realizável.
- O plano contém objetivos e cenários realistas e práticos.
- Os membros das equipes entendem o que é esperado deles nas etapas antes, durante e após o teste.

3.5. Referências legais e normativas

- Instrução Normativa Nº 01 GSIPR, de 13 de junho de 2008.
- Norma Complementar Nº 06/IN01/DSIC/GSIPR, de 11 de novembro de 2009.

4. GESTÃO DE RISCOS EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GRSIC)

A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) é conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação de um determinado órgão, e equilibrá-los com os custos operacionais e financeiros envolvidos.

Conforme a IN 01/DSIC/GSIPR, a GRSIC é uma atividade integrante da GSIC tornando-se uma atividade obrigatória e essencial para todo o Gestor de SIC.

Para implementação da SIC nos órgãos da APF, o Gestor deve seguir as recomendações contidas na Norma Complementar Nº 02/IN01/DSIC/GSIPR, baseada no processo de melhoria contínua, denominado ciclo “PDCA” (Plan-Do-Check-Act).

Na primeira fase do ciclo PDCA, denominada fase de planejamento, o Gestor de SIC planejará e implementará diversas ações de SIC:

- Definir a abordagem de gestão de riscos de seu órgão ou entidade;
- Identificar os riscos;
- Analisar os riscos;
- Identificar as opções para o tratamento de riscos;
- Selecionar as ações de SIC consideradas necessárias para o tratamento de riscos; e
- Obter aprovação da autoridade decisória de seu órgão ou entidade quanto aos riscos residuais propostos.

Com o objetivo de estabelecer diretrizes para o processo de GRSIC nos órgãos ou entidades da APF, direta e indireta, foi publicada a Norma Complementar Nº 04/IN01/GSIPR/DSIC.

Ao aplicar a GRSIC, o Gestor deve considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da APF, além de alinhar com a respectiva POSIC do órgão ou entidade.

Para que a implementação e operação da Gestão de SIC seja efetiva, torna-se importante que o Gestor implemente a GRSIC de uma forma contínua e aplicada, pois é por meio da GRSIC que o Gestor obterá subsídios necessários para suportar o SGSI, como também, para a GCN.

4.1. Procedimentos

Com a finalidade de manter os riscos em níveis aceitáveis, a abordagem sistemática do processo de GRSIC compõe as seguintes etapas:

- 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;
- Melhoria do processo de GRSIC; e
- Comunicação do risco.

A figura 5, anexa na Norma Complementar Nº 04/IN01/DSIC/GSIPR, representa como essas etapas se interagem na GRSIC:

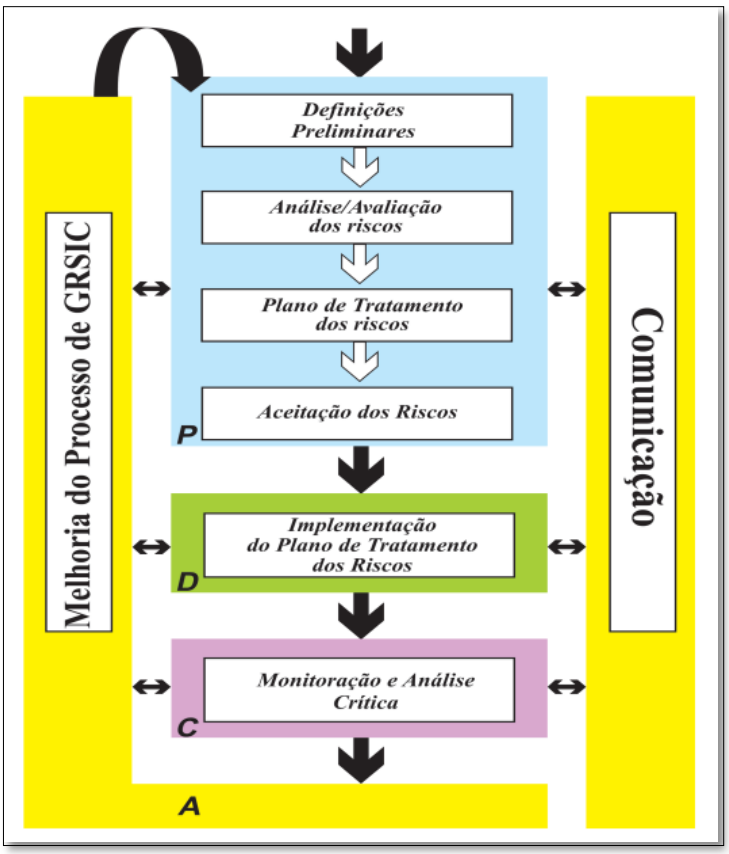

Figura 5: Anexo da Norma Complementar Nº 04/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013.

4.1.1. Definições preliminares:

Nesta fase o Gestor deve realizar uma análise da organização visando estruturar o processo de GRSIC, considerando as características e as restrições do órgão ou entidade. Esta análise inicial permite que os critérios e o enfoque da GRSIC sejam os mais apropriados para o órgão, apoiando-o na definição do escopo e na adoção de uma metodologia.

Com a finalidade de delimitar o âmbito de atuação do Gestor é preciso definir qual o escopo e onde será aplicado a GRSIC. É importante frisar que o escopo pode abranger todo o órgão, um segmento, um processo, um sistema, um recurso ou um ativo de informação.

As melhores práticas indicam que fazer a GRSIC em toda organização pode levar ao erro, assim recomenda-se inicialmente fazer a GRSIC por parte, para somente depois, já com todas as áreas mapeadas, integrar todos os escopos para uma análise total do órgão.

Após definido o escopo onde será realizado a GRSIC, o Gestor deve adotar uma metodologia de GRSIC que venha atender seus objetivos e diretrizes, bem como, o escopo definido. A Norma Complementar Nº 04/IN01/DSIC/GSIPR deixa a critério dos órgãos e entidades da APF a definição dessa metodologia, não restringindo apenas aquelas de governo, entretanto, uma vez escolhida, devem ser atendidos todos os requisitos de segurança preconizados nas normas de governo.

4.1.2. Análise/avaliação dos riscos:

Esta fase inicia-se com a análise dos riscos. Nesta fase o Gestor deve realizar o inventário e o mapeamento dos ativos de informação do escopo definido para aplicação da GRSIC, identificando as possíveis ameaças, vulnerabilidades, riscos, bem como, todas as ações de SIC já implementadas no escopo. Para a realização do inventário e mapeamento dos ativos de informação, o Gestor tem como norma balizadora a Norma Complementar Nº 10/IN01/DSIC/GSIPR.

Depois de identificados os riscos, o Gestor deve estimar os valores e os níveis de riscos, levando em consideração os fatores de probabilidade de ocorrência e também as consequências, caso aconteça, um determinado risco de segurança que venha a comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações e comunicações.

Na análise de riscos, o Gestor poderá usar as formas quantitativa e qualitativa, ou então, uma forma que utilize uma mistura dessas duas formas.

A Figura 6 representa um exemplo de Análise Qualitativa:

		Probabilidade		
		Alta	Média	Baixa
Impacto	Alto	Alto	Alto	Médio
	Médio	Alto	Médio	Baixo
	Baixo	Médio	Baixo	Baixo

Figura 6: Exemplo de Análise Qualitativa

A Figura 7 representa um exemplo de Análise Quantitativa:

		PROBABILIDADE							
		1	2	3	4	5	6	7	8
IMPACTO	1	1	2	3	4	5	6	7	8
	5	5	10	15	20	25	30	35	40
	10	10	20	30	40	50	60	70	80
	15	15	30	45	60	75	90	105	120
	20	20	40	60	80	100	120	140	160
	25	25	50	75	100	125	150	175	200

Figura 7: Exemplo de Análise Quantitativa

A Figura 8 representa um exemplo de Análise Semi-quantitativa:

		PROBABILIDADE		
		BAIXA	MÉDIA	ALTA
IMPACTO	1	10	20	30
	10	100	200	300
	100	1000	2000	3000

Figura 8: Exemplo de Análise Semi-quantitativa

Durante a fase de avaliação dos riscos, a organização estabelecerá os critérios para que os riscos sejam aceitos ou tratados. Este processo é feito por meio da comparação dos resultados obtidos na fase de análise com os critérios estabelecidos.

A Figura 9 representa um exemplo de critérios:

NÍVEL DE RISCO	DESCRIÇÃO
1 a 3	Sempre serão aceitos
4 a 6	Implementar as ações de SIC
7 a 9	Implementar **imediatamente** as ações de SIC

NÍVEL DE RISCO	DESCRIÇÃO
ALTO	Ações de SIC de implementação imediata
MÉDIO	Ações de SIC necessárias com prioridade menor
BAIXO	Não exige ação

Figura 9: Exemplo Análise de Risco

Depois de feita a análise e a avaliação dos riscos, o Gestor deve relacionar todos os riscos que requeiram tratamento, estabelecendo suas prioridades de execução em conformidade com os critérios estabelecidos.

4.1.3. Plano de Tratamento dos Riscos

Nesta fase, o Gestor determinará as formas de tratamento dos riscos encontrados, e para isso, terá quatro opções de tratamento:

- Reduzir;
- Evitar;
- Transferir; e
- Reter.

Ao definir as formas de tratamento dos riscos, o Gestor deve fazer algumas considerações relativas à eficácia das ações de SIC já existentes, às restrições existentes na organização, aos requisitos legais, e por fim, à análise de custo/benefício.

Por fim, o Gestor formulará um plano para o tratamento dos riscos, relacionando, no mínimo, as ações de SIC, os responsáveis, as prioridades e os prazos de execução necessários à sua implantação. A Figura 10 apresenta um exemplo de Plano de Tratamento:

ID	RISCO	PRIORIDADE	OPÇÕES DE TRATAMENTO	AÇÃO DE SIC	ÁREA RESPONSÁVEL	DATA FINAL

Figura 10: Exemplo de Plano de Tratamento

4.1.4. Aceitação do Risco

Nesta fase, o plano de tratamento deve ser aprovado pela alta administração do órgão. Caso haja discordância, o mesmo deve ser submetido ao Gestor para uma nova avaliação.

4.1.5. Implementação do Plano de Tratamento dos Riscos

Esta fase compreende a execução de todas as ações de SIC incluídas no Plano de Tratamento dos Riscos aprovado, cabendo ao Gestor o acompanhamento da execução dessas ações, principalmente, no que se refere a prazos.

4.1.6. Monitoração e análise crítica

Esta fase ocorre em todo o processo de GRSIC, pois é nela que todos os integrantes do processo detectam possíveis falhas nos resultados, bem como, monitorar os riscos, as ações de SIC, e por fim, verificar a eficácia do processo de GRSIC.

Cabe salientar que o monitoramento e a análise crítica incluem tanto o processo de GRSIC, como o risco propriamente dito. Isto porque, o processo deve estar alinhado às diretrizes gerais da organização, pois qualquer alteração desta altera o processo de GRSIC.

Além disso, é preciso verificar regularmente as possíveis mudanças que venham afetar as análises/avaliações dos riscos, mudanças essas que podem ser nos critérios de avaliação e aceitação dos riscos. Por exemplo, aquela probabilidade de ocorrência que anteriormente era baixa, hoje pode ser considerada alta, como uma mudança no ambiente e nos ativos de informação que alteraram o escopo que foi definido. Outra mudança pode ocorrer nas ações de SIC adotadas como as mudanças nos fatores de riscos, pois surgem cada vez mais nos dias de hoje, novas ameaças e consequentemente, novas vulnerabilidades.

4.1.7. Melhoria do Processo de GRSIC

Todas as ações detectadas na monitoração e análise crítica devem ser propostas à autoridade decisória do órgão, a fim de que sejam implementadas as devidas ações corretivas ou preventivas.

4.1.8. Comunicação do Risco

Esta fase também ocorre em todo o processo de GRSIC, é nela que todos os integrantes da GRSIC compartilham informações, principalmente entre os tomadores de decisões e demais partes.

Na fase de monitoração e análise crítica ocorrem diversas mudanças, tanto no processo de GRSIC como no risco. É por meio da comunicação que essas mudanças chegam ao conhecimento de todos os integrantes do processo.

4.2. Responsabilidades

A responsabilidade de aprovação das diretrizes de GRSIC é da alta administração do órgão, cabendo ao Gestor de SIC a coordenação da GRSIC.

Tendo em vista a complexidade da GRSIC, o Gestor de SIC poderá indicar outros servidores para auxiliá-lo em algumas atividades como na análise/avaliação de riscos e tratamento dos riscos e na elaboração de relatórios.

4.3. Referências legais e normativas

- Instrução Normativa Nº 01 GSIPR, de 13 de junho de 2008.
- Norma Complementar Nº 02/IN01/DSIC/GSIPR, de 13 de outubro de 2008.
- Norma Complementar Nº 04/IN01/DSIC/GSIPR, de 15 de fevereiro de 2013.
- Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012.

5. INFRAESTRUTURAS CRÍTICAS DA INFORMAÇÃO - ICI

A Portaria Nº 34 do Conselho de Defesa Nacional da Secretaria Executiva, que Instituiu o Grupo de Trabalho de Segurança das Infraestruturas Críticas da Informação, no âmbito do Comitê Gestor de Segurança da Informação (CGSI), define as Infraestruturas Críticas da Informação, como um 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.

5.1. ICP- BRASIL: Certificação Digital

A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), instituída pela Medida Provisória nº 2.200-2, de 24 de agosto de 2001, é uma cadeia hierárquica e de confiança que viabiliza a emissão de certificados digitais. Dentre vários modelos existentes, o modelo adotado pelo Brasil foi o de certificação com raíz única. O Instituto Nacional de Tecnologia da Informação (ITI), além de desempenhar o papel de Autoridade Certificadora Raiz (AC-Raiz), também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

A AC-Raiz executa as Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, sendo então de sua competência a função de expedir, distribuir, revogar e gerenciar os certificados das autoridades certificadoras de nível imediatamente subsequente ao seu.

A AC-Raiz também está encarregada de emitir a lista de certificados revogados (LCR) e de fiscalizar e auditar as Autoridades Certificadoras (ACs), Autoridades de Registro (ARs) e demais prestadores de serviço habilitados na ICP-Brasil. Além disso, verifica se as ACs estão atuando em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil.

O Comitê Gestor da ICP-Brasil exerce a função de autoridade gestora de políticas e encontra-se vinculado à Casa Civil da Presidência da República.

5.1.1. Conceitos Gerais

Alguns dos conceitos utilizados na ICP-Brasil são apresentados nesta seção, demais conceitos podem ser consultados no glossário disponível no endereço: <*http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Glossario/GLOSSaRIOV1.4.pdf*>

.

5.1.1.1. Algoritmo Assimétrico

É um algoritmo de criptografia que usa duas chaves: uma chave pública e uma chave privada, onde a chave pública pode ser distribuída abertamente enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia, assinaturas digitais e acordo de chave.

5.1.1.2. Assinatura Digital

Código anexado ou logicamente associado a uma mensagem eletrônica que permite de forma única e exclusiva a comprovação da autoria de um determinado conjunto de dados (um arquivo, um e-mail ou uma transação). A assinatura digital comprova que a pessoa criou ou concorda com um documento assinado digitalmente, como a assinatura de próprio punho comprova a autoria de um documento escrito. A verificação da origem do dado é feita com a chave pública do remetente.

5.1.1.3. Autenticidade

Qualidade de um documento ser o que diz ser, independente de se tratar de minuta, original ou cópia e que é livre de adulterações ou qualquer outro tipo de corrupção.

5.1.1.4. Autoridade Certificadora - AC

Entidade que emite, renova ou revoga certificados digitais de outras ACs ou de titulares finais. Além disso, emite e publica a lista de certificados revogados (LCR).

5.1.1.5. Autoridade de Carimbo de Tempo - ACT

Entidade na qual os usuários de serviços de carimbo do tempo – subscritores e terceiras parte confiam para emitir carimbos do tempo. A ACT é a responsável pelo fornecimento do carimbo do tempo.

5.1.1.6. Autoridade de Registro - AR

Entidade responsável pela interface entre o usuário e a Autoridade Certificadora vinculada a uma AC que tem por objetivo o recebimento, validação, encaminhamento de solicitações de emissão ou revogação de certificados digitais às AC e a identificação, de forma presencial, de seus solicitantes. É responsabilidade da AR manter registros de suas operações. Pode estar fisicamente localizada em uma AC ou ser uma entidade de registro remota.

5.1.1.7. Certificação Digital

Atividade de reconhecimento em meio eletrônico que se caracteriza pelo estabelecimento de uma relação única, exclusiva e intransferível entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação. Esse reconhecimento é inserido em um Certificado Digital, por uma Autoridade Certificadora.

5.1.1.8. Certificado de Atributo

Estrutura de dados contendo um conjunto de atributos (características e informações) sobre a entidade final, que é assinada digitalmente com a chave privada da entidade que o emitiu. Pode possuir um período de validade, durante o qual os atributos incluídos no certificado são considerados válidos.

5.1.1.9. Certificado Digital

Conjunto de dados de computador, gerados por uma Autoridade Certificadora, em observância à Recomendação da *International Telecommunications Union - Telecommunication Standardization Sector* - ITU-T X.509, que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave de criptografia e uma pessoa física, jurídica, máquina ou aplicação.

5.1.2. Integridade

Assegura que uma mensagem não foi alterada, excluída ou adicionada de alguma maneira durante a transmissão por uma rede, ou seja, fornece proteção contra modificações não-autorizadas, acidentais ou intencionais dos dados.

5.1.3. Não-repúdio (ou irretratabilidade)

É a garantia de que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica utilizando a certificação digital ICP-Brasil não poderá posteriormente negar sua autoria, visto que somente aquela chave privada poderia ter gerado aquela assinatura digital.

5.1.4. Arcabouço Jurídico

O arcabouço jurídico da ICP-Brasil inicia-se com a Medida Provisória nº 2.200-2, de 24 de Agosto de 2001, que instituiu a Infraestrutura de Chaves Pública Brasileira para garantir a autenticidade, a integridade e a validade jurídica aos documentos em forma eletrônica, as aplicações de suporte e as aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Dentre os vários Decretos relacionados ao tema, cabe destacar o Decreto Nº 3.996, de 31 de outubro de 2001, que dispõe sobre a prestação de serviços, cujos serviços a serem prestados, credenciados ou contratados pelos órgãos e entidades da APF devem ser promovidos no âmbito da ICP-Brasil. Neste contexto, a tramitação de documentos eletrônicos, as aplicações e demais programas e equipamentos utilizados no âmbito da APF, direta e indireta, que exijam a utilização de certificados digitais será mediante certificação disponibilizada por AC integrante da ICP-Brasil.

A legislação vigente pode ser consultada no site do ITI no endereço: <*http://www.iti.gov.br/index.php/icp-brasil/legislacao*>.

5.2. Referências sobre ICI

Para melhor compreensão pelos gestores sobre o assunto, o Departamento de Segurança da Informação e Comunicações do GSI / PR publicou em 2010 o Guia de Referência Para a Segurança das Infraestruturas Críticas da Informação. Disponível em formato eletrônico no sítio eletrônico: http://dsic.planalto.gov.br.

5.3. Referências legais e normativas

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