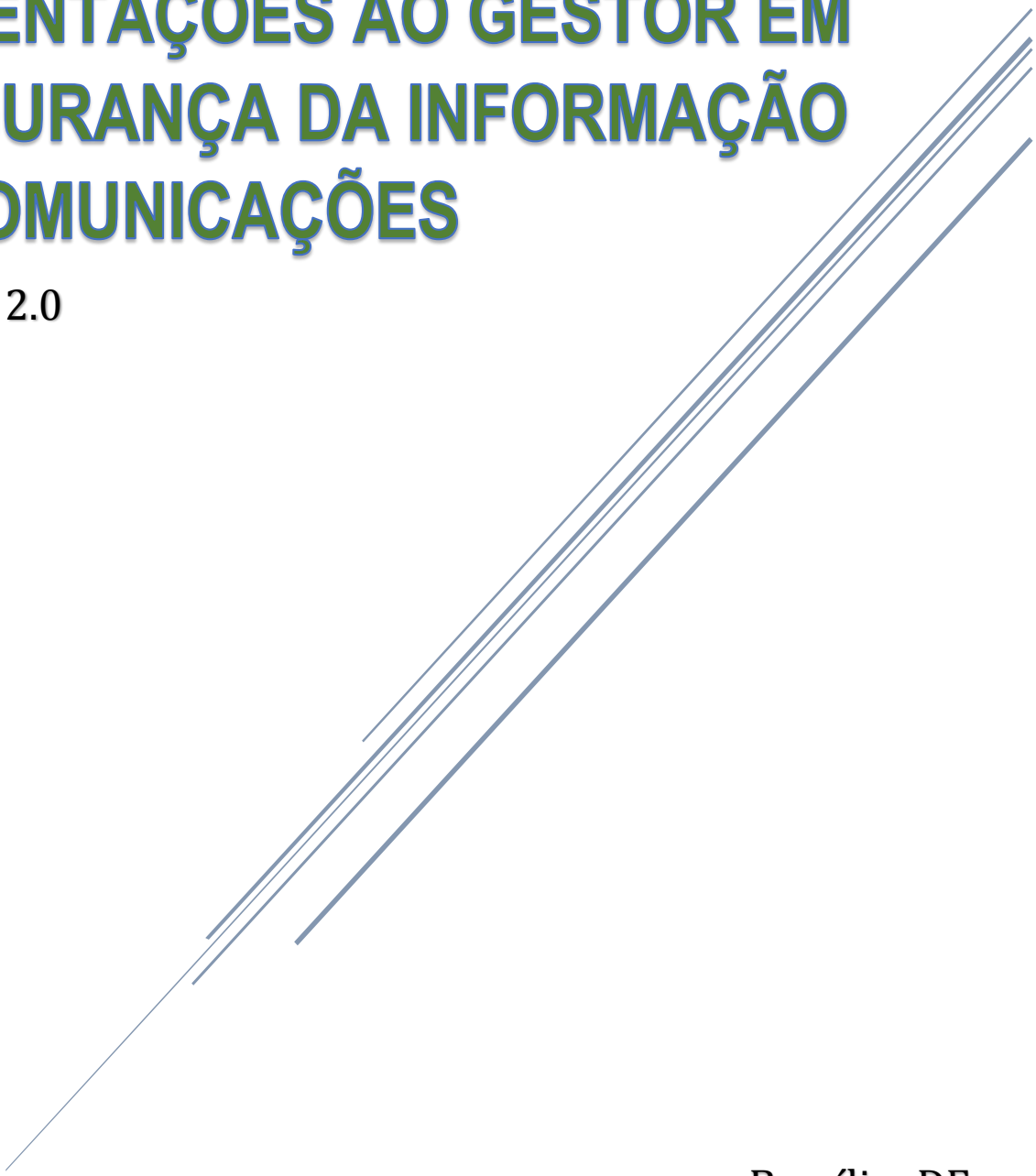
GUIA BÁSICO DE ORIENTAÇÕES AO GESTOR EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Versão 2.0



Brasília- DF
2015

Presidenta da República
Dilma Rousseff

Vice-Presidente da República
Michel Temer

Chefe da Casa Militar da Presidência da República
General de Divisão Marcos Antonio Amaro dos Santos

Secretário-Executivo do Conselho de Defesa Nacional
General de Divisão Marcos Antonio Amaro dos Santos

Assessor-Chefe da Assessoria Especial da Secretaria-Executiva do Conselho de Defesa Nacional
Contra-Almirante Noriaki Wada

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

Coordenador do Comitê Gestor da Segurança da Informação
Marconi dos Reis Bezerra

PRESIDÊNCIA DA REPÚBLICA
Casa Militar
Secretaria-Executiva do Conselho de Defesa Nacional
Departamento de Segurança da Informação e Comunicações

GUIA BÁSICO DE ORIENTAÇÕES AO GESTOR EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Versão 2.0

Brasília – DF
2015

Disponível no formato eletrônico em: <*http://dsic.planalto.gov.br*>.

Organizadores

Danielle Rocha da Costa

José Ney de Oliveira Lima

Membros do GT

Adelino Fernando de Souza Correia, *Ministério da Saúde*

Carlos de Faria Castro*, Ministério da Previdência Social*

Danielle Rocha da Costa, *Gabinete de Segurança Institucional da Presidência da República*

Eduardo Magalhães de Lacerda Filho, *Casa Civil da Presidência da República*

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*

Lucas de Oliveira Souto, *Gabinete de Segurança Institucional da Presidência da República*

Marlene Isidro da Silva, *Gabinete de Segurança Institucional da Presidência da República*

Marcos Allemand Lopes, *Ministério da Fazenda*

Núbia Moreira dos Santos, *Ministério do Planejamento, Orçamento e Gestão*

Zeneide Sanches Pureza *(Convidada), Secretaria de Segurança Pública e Defesa Social do Estado do Pará*

Normalização bibliográfica: Biblioteca da Presidência da República.

Desenvolvido pelo Grupo de Trabalho (GT) – **"Elaboração de Guia de Orientações ao Gestor de SIC"**, instituído no âmbito do Comitê Gestor da Segurança da Informação (CGSI), por meio da Portaria Nº 26 do Conselho de Defesa Nacional (CDN), de 15 de Julho de 2014.

[Membros designados pela **Portaria Nº 28 SE/CDN, de 7 de Agosto de 2014 -** (DOU nº 151; 8/08/2014)]

Ficha Catalográfica

Dados Internacionais de Catalogação na Publicação (CIP)

B823g
Brasil. Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações.
Guia básico de orientações ao gestor em segurança da informação e comunicações : versão 2.0 / Casa Militar, Departamento de Segurança da Informação e Comunicações; organizadores Danielle Rocha da Costa, José Ney de Oliveira Lima. – Brasília : Presidência da República, 2016.
92 p. : il.

1. Segurança da informação e comunicações. 2. Gestão em segurança da informação e comunicações. I. Título.

CDD 005.8

Ficha Catalográfica produzida pela Biblioteca da Presidência da República

SUMÁRIO

LISTA DE SIGLAS

ACs	Autoridades Certificadoras
AIN	Análise de Impacto nos Negócios
APF	Administração Pública Federal
CTIR GOV	Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal
DICA	Disponibilidade, Integridade, Confidencialidade e Autenticidade
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
GSIC	Gestão da Segurança da Informação Comunicações
ICP- Brasil	Infraestrutura de Chaves Públicas Brasileira
ITI	Instituto Nacional de Tecnologia da Informação
POSIC	Política de Segurança da Informação e Comunicações
SE/CDN	Secretária-Executiva do Conselho de Defesa Nacional
SGCN	Sistema de Gestão de Continuidade de Negócios
SIC	Segurança da Informação e Comunicações
TIC	Tecnologia da Informação e Comunicações

LISTA DE FIGURAS

LISTA DE TABELAS

APRESENTAÇÃO

É com imensa satisfação que apresento este Guia Básico 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 para publicação desta obra, tem-se a própria prerrogativa do Secretário Executivo do Conselho de Defesa Nacional de coordenar a implantação da Política de Segurança da Informação no Governo Federal, bem como a respectiva competência de coordenar o Comitê Gestor da Segurança da Informação (CGSI) que, entre outras atividades, normatiza a Segurança da Informação e Comunicações no âmbito da Administração Pública Federal (APF), mantendo o compromisso do Estado de promover ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Dessa forma, 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 APF.

Este Guia Básico de Orientações, além de assistir a missão da SE/CDN, 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 2014 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 grupo foi composto por 12 servidores federais dos seguintes órgãos à época: GSIPR, 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 da Informação, 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! Boas práticas!

General de Divisão Marcos Antonio Amaro dos Santos

Chefe da Casa Militar da Presidência da República

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 Básico 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 este estudo adotou como referencial 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) no período de maio de 2006 a setembro de 2015, disponíveis no sítio: <https://dsic.planalto.gov.br/>.

Dessa forma, esse 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 e 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 - GRSIC:** 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.

- **Infraestrutura de Chaves Públicas Brasileira-ICP-BRASIL:** anexo a este Guia, trata sobre a cadeia hierárquica e de confiança da ICP-BRASIL que viabiliza a emissão de certificados digitais.

- **Glossário de SIC:** um Glossário com conceitos e definições oriundos dos Normativos publicados pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR) é apresentado ao final deste estudo compreendo todos os conceitos publicados na Instrução Normativa GSI Nº 1, de 13 de junho de 2008, e suas respectivas 21 Normas Complementares, de maio de 2008 à outubro de 2014.

Esse Guia 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

Elaboração de Guia de Orientações ao Gestor de SIC

CONTEXTUALIZAÇÃO

As diretrizes e metas relacionadas ao tema Segurança da Informação e 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, igualmente na tomada de decisões estratégicas, as ações exercidas possuem estreito relacionamento com a segurança da informação e comunicações. Problemas decorrentes da falta de *Disponibilidade, Integridade, Confidencialidade e Autenticidade (DICA)* em sistemas de informação levam à necessidade de desenvolver ações permanentes e gradativas nas organizações da APF. Diante desse cenário, surgem vários 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 escopo 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 Resposta 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, a Política de Segurança da Informação e Comunicações (POSIC) e os normativos vigentes.

Ressalta-se a obrigatoriedade do arcabouço normativo de SIC publicado pelo GSI/PR, do mesmo modo que tal aplicação/implantação do citato arcabouço nos órgãos e entidades da APF é de responsabilidade da Alta Administração, conforme Acórdão 1233/2012 – TCU-Plenário. Portanto, nesta versão 2.0 deste Guia tratamos de quatro temas fundamentais no contexto da SIC:

- ***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); e***
- ***Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC).***

Considerando o panorama exposto, este Guia visa prover ao Gestor conhecimentos básicos necessários para conduzir e planejar as ações de SIC. Observa-se que no escopo da APF, as "boas práticas" de SIC são as ações de segurança da informação e comunicações descritas no arcabouço normativo desenvolvido pelo DSIC/GSIPR, cuja observância é obrigatória e de responsabilidade da Alta Administração da APF, conforme Acórdão 1.233/2012-TCU-Plenário em relação aos normativos de SIC publicados pelo GSI/PR.

Além disso, compete aos Gestores de SIC articular e promover o planejamento das ações de segurança da informação e comunicações nos órgãos e entidades da APF como previsto na Norma Complementar Nº 02/IN01/DSIC/GSIPR, devidamente alinhado tanto aos requisitos e pressupostos estabelecidos pelo planejamento estratégico do órgão bem como ao disposto na *"Estratégica de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015/2018, versão 1.0".*

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

A POSIC é um documento estratégico que compreende um conjunto de diretrizes com vistas a promover o uso seguro dos ativos de informação de uma organização. Deste modo, a POSIC pode 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 relacionados somente aos aspectos tecnológicos.

Neste contexto, uma POSIC declara o comprometimento da alta direção organizacional com as ações de segurança da informação e comunicações, além de prover diretrizes estratégicas, responsabilidades, competências e apoio para implementar a Gestão da Segurança da Informação Comunicações (GSIC).

Além do mais, o estabelecimento de suas diretrizes objetiva viabilizar e assegurar a D*isponibilidade, Integridade, Confidencialidade e Autenticidade* (DICA) das informações no âmbito da APF, direta e indireta.

Disponibilidade

Diz respeito à garantia de que a informação estará acessível às pessoas, processos automatizados, órgãos ou entidades no momento que for requerida. Logo, a

disponibilidade está relacionada à prestação continuada de um serviço, sem interrupções no fornecimento de informações.

Integridade

A integridade da informação está relacionada à sua fidedignidade. Assegurar a integridade da informação, portanto, significa garantir que a informação não foi modificada ou destruída de maneira não autorizada, quer de forma acidental ou intencional.

Confidencialidade

Implica em impedir o acesso não autorizado, quer acidental quer intencional, garantindo que apenas pessoas, sistemas, órgãos ou entidades devidamente autorizados e credenciados tenham acesso à informação.

Autenticidade

Mediante a autenticação é possível confirmar a identidade de quem presta a informação. Ou seja, a autenticação permite assegurar a fidedignidade da fonte da informação.

1.2.1. Responsabilidades

É da competência da Alta Administração dos órgãos e entidades da APF avaliar a necessidade de que na estrutura da organização exista uma área responsável pela segurança da informação e comunicações.

Cabe ao Gestor de SIC a responsabilidade pela elaboração da POSIC, assessorado pelo Comitê Gestor de SIC do órgão, bem como pela sua implantação e revisão após aprovação da referida pela Alta Administração.

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 respectivas 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, portanto, 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/PR 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 sua implementação; e
- Promover no órgão ou entidade a cultura de segurança da informação por meio de atividades de sensibilização, conscientização, capacitação e especialização.

É importante salientar que 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, todos

os instrumentos normativos gerados a partir da POSIC, inclusive a 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

A Tabela 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 de SIC alinhado ao planejamento estratégico do órgão e entidade da APF pautado nas características específicas dos mesmos. *Considerar o contexto da organização, mapear os ativos de informação e avaliar o que deve ser protegido.* **2. Promover a aprovação da POSIC pela alta direção do órgão.** *O patrocínio da alta administração é fundamental para o sucesso na adoção da POSIC.* **3. Efetuar mapeamento e análise dos ativos de informação do órgão e entidade da APF.** *Definir os níveis e requisitos de segurança a serem aplicados conforme a criticidade e relevância de cada ativo de informação. 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. 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 – assim 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-Recomendações 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 a finalidade do órgão ou entidade, considerando sua missão e planejamento estratégico. De acordo 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

Compete à Alta Administração dos órgãos e entidades da APF:

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

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 conforme apresenta a Figura 1.

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

Recomenda-se a normatização dos respectivos assuntos já publicados pelo GSI/PR e portanto obrigatórios, envolvendo as áreas de tecnologia, pessoas, ambiente e processos. Além disso, sugere-se que temas ainda não normatizados no governo federal, mas já amparados por normas da família ISSO 27.0001/27.0002, também sejam analisados a luz das necessidades específicas de cada órgão e entidade da APF:

1) Planejamento e Gestão de SIC;

2) Tratamento da Informação;

3) Formação de Equipes de Tratamento de Incidentes de Segurança em Redes Computacionais;

4) Gerenciamento de Incidentes de Segurança em Redes Computacionais;

5) Inventário e mapeamento de ativos de informação;

6) Gestão de Riscos nos aspectos de SIC;

7) Gestão de mudanças nos aspectos relativos à SIC;

8) Gestão de Continuidade de Negócios nos aspectos de SIC;

9) Avaliação e Conformidade de SIC;

10) Controles de Acesso relativos à SIC;

11) Uso seguro de Dispositivos móveis;

12) Uso seguro de Computação em nuvem;

13) Uso seguro de Redes Sociais;

14) Desenvolvimento e obtenção de software seguro;

15) Atuação e adequações para profissionais da área de SIC;

16) Atividades de ensino em SIC;

17) SIC em Sistemas Estruturantes;

18) Uso de recursos criptográficos;

19) Registro de eventos, coleta e preservação de evidências de incidentes de segurança;

20) Uso seguro de e-mail;

21) Backup; e

22) Uso seguro da Internet.

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 Resposta 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 deforma 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 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.

2.2.3. 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, em conformidade com o 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/DSIC.

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/DSIC, conforme procedimentos normatizados pelo GSI/PR, específicos sobre o assunto.

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

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

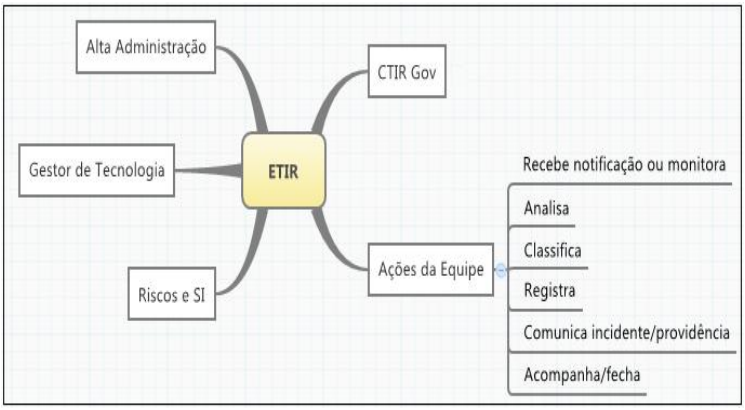


Figura 2: Todo o processo deve ser balizado pelas Normas Complementares Nº 05 e Nº 08 da IN01/DSIC/GSIPR.

2.4. Resultados esperados

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

⇒ 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;

⇒ Composição de séries históricas como subsídio estatístico; e

⇒ Articulação com o CTIR Gov/DSIC.

2.5. Etapas para alcance dos resultados

2.5.1. 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 da criticidade dos ativos de informação do órgão ou entidade;

d) Conhecimento do nível de maturidade e sensibilização dos servidores e colaboradores de TIC em relação ao tema;

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

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

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

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

Recomenda-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.

2.5.3. Opções recomendadas

2.5.3.1. Modelos

1. Estruturado como componente da área 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.

2.5.3.2. 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.

2.5.3.3. 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.

2.6. 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.
- NIC.br - Núcleo de Informação e Coordenação do Ponto BR Disponível em: <*http://www.nic.br*>.

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

A Gestão de Riscos em Segurança da Informação e Comunicações (GRSIC) é um 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 Gestão de SIC tornando-se uma atividade obrigatória e essencial para todo o Gestor de SIC. Convém que o processo de GRSIC esteja alinhado ao planejamento estratégico da organização e também, com o processo maior de gestão de riscos corporativos, se esse existir.

Para implementação da SIC nos órgãos e entidades 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 como:

- 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 foi publicada a Norma Complementar Nº 04/IN01/GSIPR/DSIC

(Revisão 01). Ao aplicar a supracitada Norma, 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, pois é por meio da GRSIC que o Gestor obterá subsídios necessários para suportar um Sistema de Gestão de Segurança da Informação (SGSI), como também a GCN.

3.1. Procedimentos

Com a finalidade de manter os riscos em níveis aceitáveis a abordagem sistemática do processo de GRSIC compreende 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 Norma Complementar Nº 04/IN01/DSIC/GSIPR (Revisão 01), em seu Anexo, apresenta a interação das etapas da GRSIC.

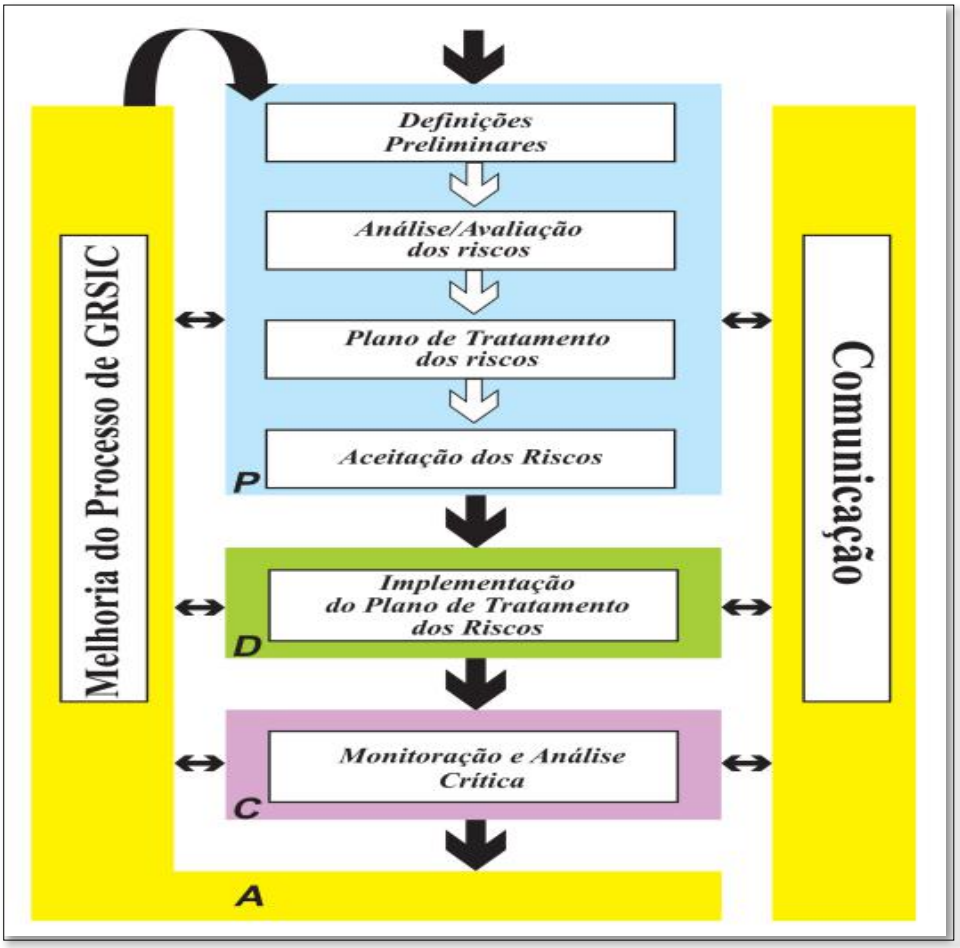


Figura 3: Anexo da NC Nº 04/IN01/DSIC/GSIPR (Revisão 01)

3.1.1. Definições preliminares

Na fase de definição preliminares 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-se na definição do escopo e na adoção de uma metodologia.

Com a finalidade de delimitar o âmbito de atuação do Gestor é preciso definir 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, após o mapeamento de todas as áreas realizar a integração de todos os escopos previamente elaborados para uma análise total do órgão.

Dessa forma, após definido o escopo onde será realizado a GRSIC, o Gestor deve adotar uma metodologia de GRSIC que venha atender aos seus objetivos e diretrizes. A Norma Complementar Nº 04/IN01/DSIC/GSIPR (Revisão 01), deixa a critério dos órgãos e entidades da APF a definição dessa metodologia, não restringindo apenas aquelas de governo. Todavia, uma vez escolhida a metodologia, devem ser atendidos todos os requisitos de segurança preconizados nas normas de governo.

3.1.2. 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 definidos no escopo para aplicação da GRSIC, identificando as possíveis ameaças, vulnerabilidades, riscos, tal como todas as ações de SIC já implementadas no escopo. Para a realização do inventário e mapeamento dos ativos de informação, a Norma Complementar Nº 10/IN01/DSIC/GSIPR fornece subsídios para realização do processo de Inventário e Mapeamento de Ativos de Informação para o órgão ou entidade da APF, em conformidade com os requisitos legais e do negócio. Esse processo de Inventário e Mapeamento de Ativos de Informação deve ser dinâmico, periódico e estruturado com a finalidade de manter a Base de Dados de Ativos de Informação atualizada e, conseqüentemente, prover informações para o desenvolvimento de ações e planos de aperfeiçoamento de práticas de Gestão da Segurança da Informação e Comunicações.

Dessa maneira, 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, de um determinado risco de segurança comprometer a disponibilidade, integridade, confidencialidade e autenticidade das informações.

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 4: Exemplo de Análise Qualitativa

A Figura 7 apresenta um outro 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 5: Exemplo de Análise Quantitativa

A Figura 8 demonstra um exemplo de Análise Semi-quantitativa

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

Figura 6: 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. Esse processo é feito por meio da comparação dos resultados obtidos na fase de análise com os critérios estabelecidos.

A Figura 9 expõe 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 7: 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.

3.1.3. Plano de Tratamento dos Riscos

Nesta fase, o Gestor determinará as formas de tratamento dos riscos identificados. Diante disso, cabe observar as 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, realizar a análise de custo/benefício.

Portanto, 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.

3.1.4. Aceitação do Risco

A Figura 10 apresenta um modelo de plano de tratamento. Após a adoção de um modelo o mesmo deve ser aprovado pela alta administração do órgão. Caso haja discordância no plano de tratamento proposto, o mesmo deve ser submetido ao Gestor para uma nova avaliação.

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

Figura 8: Exemplo de Plano de Tratamento

3.1.5. Implementação do Plano de Tratamento dos Riscos

Esta etapa 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, em relação aos prazos.

3.1.6. Monitoração e análise crítica

Nesta fase ocorre todo o processo de GRSIC. Os integrantes que fazem parte desse processo detectam possíveis falhas nos resultados, monitoram os riscos, as ações de SIC e por fim, verificam a eficácia da 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. Essas mudanças podem ser nos critérios de avaliação e aceitação dos riscos, por exemplo, uma probabilidade de ocorrência que anteriormente era baixa, no momento atual pode ser considerada alta, como uma mudança no ambiente que altera o escopo que foi anteriormente definido. Outra mudança que pode ocorrer nas ações de SIC são os fatores de riscos, pois surgem cada vez mais, novas ameaças e, consequentemente, novas vulnerabilidades.

3.1.7. 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.

3.1.8. 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 as 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.

3.2. Responsabilidades

A responsabilidade da 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, no tratamento dos riscos e na elaboração de relatórios.

3.3. 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, e seu anexo (Revisão 01) de 15 de fevereiro de 2013.
- Norma Complementar Nº 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012.

4. GESTÃO DE CONTINUIDADE DE NEGÓCIOS

4.1. 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.

4.2. 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	RESPONSABILIDADES
Alta Administração	· Assegurar a existência da gestão de 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 definidas. · Delegar as atividades de planejamento e coordenação do processo de gestão de continuidade ao Gestor de Continuidade de Negócios. · Conceder ao Gestor de Continuidade de Negócios a devida autoridade.
Gestor/Coordenador de GCN	· Posicionar a Alta Administração sobre a evolução do Sistema de Gestão de Continuidade de Negócios (SGCN). · Posicionar a Alta Administração sobre a evolução da situações de emergência / contingência local e regionais. · Planejar e coordenar a realização dos testes / exercícios corporativos. · Participar do Comitê Gestor de Segurança da Informação e Comunicações do órgão ou entidade. · Coordenar o desenvolvimento/manutenção dos planos setoriais / 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 Gestor de Segurança da Informação e Comunicações do órgão ou entidade	· Revisar aspectos estratégicos da GCN. · Manter o SGCN. · Apoiar o Gestor/Coordenador nas situações de emergência/ desastre. · Aprovar os planos corporativos. · Coordenar o desenvolvimento/manutenção dos planos setoriais / regionais. · Coordenar a elaboração/execução dos testes e exercícios setoriais/ regionais.

Tabela 1: Papéis e Responsabilidades na GCN.

4.3. Resultados esperados

A implantação do processo de GCN 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
Início 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.
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).
	Política de continuidade de negócios.

Desenvolver e implementar uma resposta de GCN	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 2: Etapas do projeto GCN – Visão geral.

4.4. Etapas para o alcance dos resultados

4.4.1. Entender a Organização – Análise de Riscos

A análise de riscos realizada no contexto da GCN 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.

4.4.2. 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 e 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. Assim, a AIN é um processo para analisar as funções de negócios e os efeitos que uma interrupção pode causar sobre as mesmas.

Objetivos da AIN:

- 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, porém os impactos devem estar relacionados aos objetivos de negócio e às partes interessadas da organização como:

- 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.
- Analisar as funções de negócio e os efeitos que uma interrupção possa causar nelas.
- 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, como também 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 SIC para que os objetivos de recuperação sejam atingidos nos prazos estabelecidos.

Os Requisitos de tempos de recuperação (janelas de tempos), importantes para a AIN nas situações de recuperação de desastres de TI (Disaster Recovery) são ilustrados na tabela 4 e na 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;
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 3: Tempos a serem considerados no plano de recuperação de desastres.

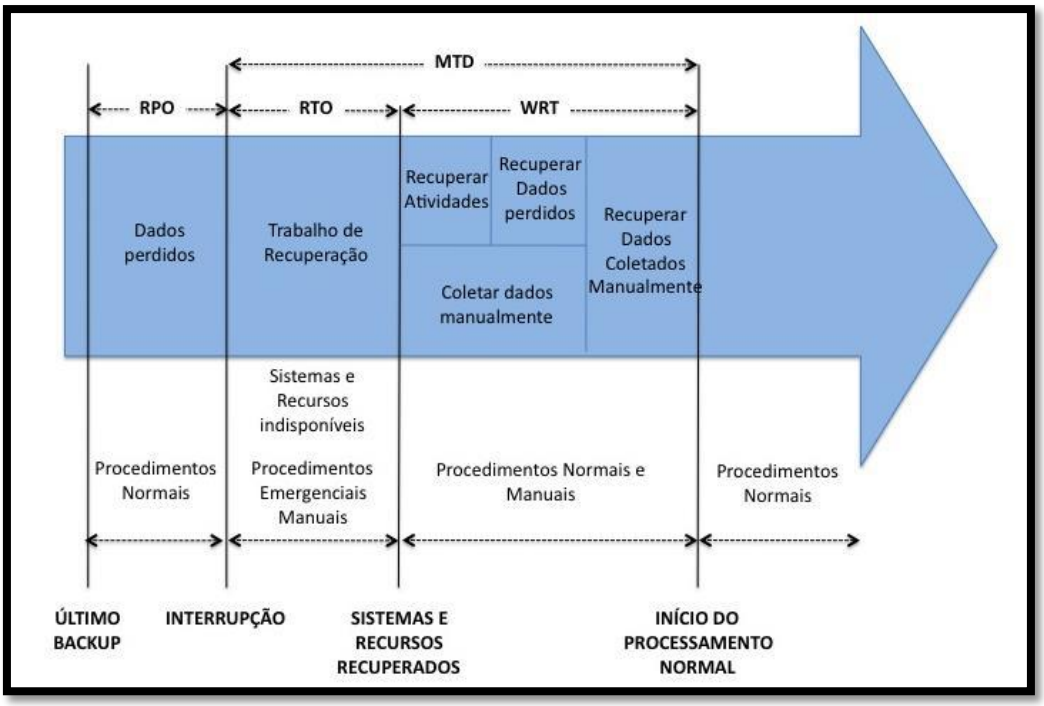


Figura 9: Tempos associados com o plano de recuperação de desastres de TI.

4.4.3. 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).

4.4.4. Desenvolver e Implementar uma Resposta de GCN

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

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.

As seguintes atividades devem ser conduzidas nesta etapa do trabalho:

- 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 aspectos devem ser considerados no desenvolvimento das atividades:

- 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).

4.4.5. 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 SIC.

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 Recuperação de Negócios	Documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.

Tabela 4: Tipos de planos de acordo com a Norma Complementar Nº 06/IN01/DSIC/GSIPR

4.4.6. 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

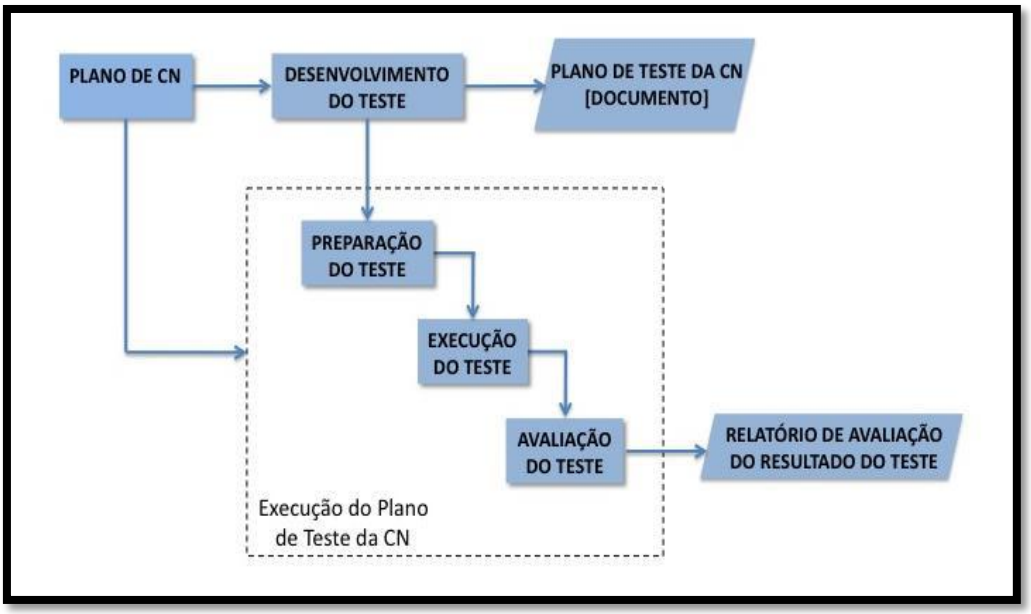


Figura 10: Etapas de execução do teste do plano de continuidade de negócios.

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.

- 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 5: 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.

4.5. 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.

GLOSSÁRIO DE SIC

A

ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

ADMINISTRADOR DE PERFIL INSTITUCIONAL: agentes públicos que detenham autorização do responsável pela área interessada para administrar perfis institucionais de um órgão ou entidade da APF nas redes sociais.
https://dsic.planalto.gov.br/documentos/nc_15_redes_sociais.pdf

AGENTE PÚBLICO: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da APF.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

AGENTE PÚBLICO COM DISPOSITIVO MÓVEL CORPORATIVO: servidores ou empregados da APF, que utilizam dispositivos móveis de computação de propriedade dos órgãos ou entidade a que pertencem.
http://dsic.planalto.gov.br/documentos/nc_12_dispositivos.pdf

AGENTE PÚBLICO COM DISPOSITIVO MÓVEL PARTICULAR: servidores ou empregados da APF que utilizam dispositivos móveis de computação de sua propriedade.
http://dsic.planalto.gov.br/documentos/nc_12_dispositivos.pdf

AGENTE RESPONSÁVEL (CREDENCIAMENTO): servidor público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade do Poder Executivo Federal e possuidor de credencial de segurança.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

AGENTE RESPONSÁVEL PELA ETIR: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

AGENTE RESPONSÁVEL (GESTÃO DE ATIVOS): Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta, incumbido de chefiar e gerenciar o processo de Inventário e Mapeamento de Ativos de Informação.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

ALGORITMO DE ESTADO: função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente as informações classificadas, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, não comercializável.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

ALGORITMO REGISTRADO: função matemática utilizada na cifração e na decifração de informações não classificadas, para uso exclusivo em interesse do serviço de órgãos ou entidades da APF, direta e indireta, cujo código fonte e método de processos sejam passíveis de controle e auditoria.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

AMBIENTAÇÃO: Evento que oferece informações sobre a missão organizacional do órgão ou instituição, bem como sobre o papel do agente público nesse contexto.

http://dsic.planalto.gov.br/documentos/nc_18_atividades_ensino.pdf

AMEAÇA – conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

ANÁLISE DINÂMICA: tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de interações com o software em execução.
http://dsic.planalto.gov.br/documentos/nc_16_software_seguro.pdf

ANÁLISE ESTÁTICA: tipo de teste de software que verifica sua lógica interna em busca de falhas ou vulnerabilidades. A análise estática ocorre por meio da verificação do código-fonte ou dos binários.
http://dsic.planalto.gov.br/documentos/nc_16_software_seguro.pdf

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 órgão 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 SIC para que os objetivos de recuperação sejam atendidos nos prazos estabelecidos.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

ANÁLISE DE RISCO: uso sistemático de informações para identificar fontes e estimar o risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

AQUISIÇÃO DE EVIDÊNCIA: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

ARTEFATO MALICIOSO: é 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.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

ATIVIDADE: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

ATIVIDADES CRÍTICAS: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

ATIVIDADE DE ENSINO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: eventos de orientação/instrução que abordam o tema SIC.
http://dsic.planalto.gov.br/documentos/nc_18_atividades_ensino.pdf

ATIVOS DE INFORMAÇÃO: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

AUDITORIA: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

AUTENTICAÇÃO: processo de identificação das partes envolvidas em um processo.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

AUTENTICAÇÃO DE MULTIFATORES: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, tokens, códigos enviados por SMS e similares) ou algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros).
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

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.
http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

AUTORIZAÇÃO: processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

AVALIAÇÃO DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: exame sistemático do grau de atendimento dos requisitos relativos à SIC com as legislações específicas.
http://dsic.planalto.gov.br/documentos/nc_11_conformidade.pdf

AVALIAÇÃO de RISCO: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

B

BIOMETRIA: é a verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

BLOQUEIO DE ACESSO: processo que tem por finalidade suspender temporariamente o acesso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

C

CAPACITAÇÃO: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema, estando aptos para atuar em suas organizações como Gestores de SIC.
http://dsic.planalto.gov.br/documentos/nc_18_atividades_ensino.pdf

CERTIFICAÇÃO PROFISSIONAL: processo negociado pelas representações dos setores sociais, pelo qual se identifica, avalia e valida formalmente os conhecimentos, saberes, competências, habilidades e aptidões profissionais desenvolvidos em programas educacionais ou na experiência de trabalho, com o objetivo de promover o acesso,

permanência e progressão no mundo do trabalho e o prosseguimento ou conclusão de estudos.
http://dsic.planalto.gov.br/documentos/nc_17_profissionais_sic.pdf

CICLO DE VIDA DA INFORMAÇÃO: ciclo formado pelas fases da Produção e Recepção; Registro e Armazenamento; Uso e Disseminação; e Destinação.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

CIFRAÇÃO: ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem em claro, por outros ininteligíveis por pessoas não autorizadas a conhecê-la.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

CHAVE CRIPTOGRÁFICA: valor que trabalha com um algoritmo criptográfico para cifração ou decifração.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

COLETA DE EVIDÊNCIAS DE SEGURANÇA EM REDES COMPUTACIONAIS: Processo de obtenção de itens físicos que contém uma potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Este processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

COMUNICAÇÕES DO RISCO: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas. http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

COMUNIDADE OU PÚBLICO ALVO: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

COMPUTAÇÃO EM NUVEM: modelo computacional que permite acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços.
http://dsic.planalto.gov.br/documentos/nc_14_nuvem.pdf

CONFIDENCIALIDADE: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.
http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: cumprimento das legislações, normas e procedimentos relacionados à segurança da informação e comunicações da organização.
http://dsic.planalto.gov.br/documentos/nc_11_conformidade.pdf

CONSCIENTIZAÇÃO: atividade de ensino que tem como objetivo orientar sobre o que é SIC, fazendo com que os participantes saibam aplicar os conhecimentos em sua rotina pessoal e profissional, além de servirem como multiplicadores sobre o tema.
http://dsic.planalto.gov.br/documentos/nc_18_atividades_ensino.pdf

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.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

CONTAS DE SERVIÇO: contas de acesso à rede corporativa de computadores, necessárias a um procedimento automático (aplicação, script, etc) sem qualquer intervenção humana no seu uso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

CONTROLES DE SEGURANÇA: medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: a criptografia, as funções de “hash”, a validação de entrada, o balanceamento de carga, as trilhas de auditoria, o controle de acesso, a expiração de sessão, os “backups”, etc.
http://dsic.planalto.gov.br/documentos/nc_16_software_seguro.pdf

CONTÊINERES DOS ATIVOS DE INFORMAÇÃO: o contêiner é o local onde “vive” o ativo de informação, onde está armazenado, como é transportado ou processado.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

CREDENCIAIS OU CONTAS DE ACESSO: permissões, concedidas por autoridade competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

CREDENCIAL DE SEGURANÇA: certificado que autoriza pessoa para o tratamento de informação classificada.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

CREDENCIAMENTO: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

CUSTODIANTE: aquele que, de alguma forma e total ou parcialmente, zela pelo armazenamento, operação, administração e preservação de um sistema estruturante – ou de ativos de informação que compõem um estruturante – que não lhe pertence, mas que está sob sua custódia.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

CUSTODIANTE DO ATIVO DE INFORMAÇÃO: refere-se a qualquer indivíduo ou estrutura do órgão ou entidade da APF que tenha a responsabilidade formal de proteger um ou mais ativos de informação, como é armazenado, transportado e processado, ou seja, é o responsável pelos contêineres dos ativos de informação. Consequentemente, o custodiante do ativo de informação é responsável por aplicar os níveis de controles de segurança em conformidade com as exigências de segurança da informação e comunicações comunicadas pelos proprietários dos ativos de informação.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

D

DECIFRAÇÃO: ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

DESASTRE: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

DISPONIBILIDADE: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

DISPOSITIVOS MÓVEIS: consiste em equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória.
http://dsic.planalto.gov.br/documentos/nc_12_dispositivos.pdf

E

EMPRESA ESTRATÉGICA DE DEFESA (EED) DO SETOR DE TECNOLOGIA DE INFORMAÇÃO E COMUNICAÇÃO (TIC): toda pessoa jurídica do setor de Tecnologia de

Informação e Comunicação (TIC) devidamente credenciada pelo Ministério da Defesa mediante o atendimento cumulativo das condições previstas no inciso IV do art. 2º da Lei nº 12.598, de 22 de março de 2012.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

ENDEREÇO IP (Internet Protocol): refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

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 computadores.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

ESTRATÉGIA DE CONTINUIDADE DE NEGÓCIO: abordagem de um órgão ou entidade que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou outro incidente maior.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

ESTIMATIVA DE RISCO: processo utilizado para atribuir valores à probabilidade e consequências de um risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

EVIDÊNCIA DIGITAL: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

EVITAR RISCO: uma forma de tratamento de risco na qual a alta administração decide não realizar a atividade, a fim de não se envolver ou agir de forma a se retirar de uma situação de risco.

http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

EXCLUSÃO DE ACESSO: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

G

GESTÃO DE CONTINUIDADE: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. 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.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

GESTÃO DE MUDANÇA NOS ASPECTOS RELATIVOS À SIC: é o processo de gerenciamento de mudanças, de modo que ela transcorra com mínimos impactos no âmbito do órgão ou entidade da APF, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.
http://dsic.planalto.gov.br/documentos/nc_13_mudancas.pdf

GESTOR DE MUDANÇAS: é o responsável pelo processo de mudanças no âmbito do órgão ou entidade da APF.
http://dsic.planalto.gov.br/documentos/nc_13_mudancas.pdf

GESTÃO DE RISCO DE SEGURANÇA DE INFORMAÇÃO E COMUNICAÇÕES: conjunto de processos que permitem 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.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

GESTÃO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações.
http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

GESTOR DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: é o responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da APF.
http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

I

IDENTIFICAÇÃO E CLASSIFICAÇÃO DE ATIVOS DE INFORMAÇÃO: é um processo composto por 6 (seis) etapas:
(a) coletar informações gerais;
(b) definir as informações dos ativos;
(c) identificar o(s) responsável (is);
(d) identificar os contêineres dos ativos;
(e) definir os requisitos de segurança; e
(f) estabelecer o valor do ativo de informação.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

IDENTIFICAÇÃO DE RISCO: processo para localizar, listar e caracterizar elementos do risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

INCIDENTE: evento que tenha causado algum dano, colocado em risco, algum ativo de informação crítico ou interrompido a execução de alguma z
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

INCIDENTE DE SEGURANÇA: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

INCIDENTE DE SEGURANÇA EM REDES COMPUTACIONAIS: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

INFORMAÇÃO CLASSIFICADA: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, a qual é classificada como ultrassecreta, secreta ou reservada.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

INFRAESTRUTURA CRÍTICA DA INFORMAÇÃO: são os 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.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

INTEGRIDADE: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

INVENTÁRIO E MAPEAMENTO DE ATIVOS DE INFORMAÇÃO: é um processo interativo e evolutivo, composto por 3 (três) etapas:
(a) identificação e classificação de ativos de informação;
(b) identificação de potenciais ameaças e vulnerabilidades; e
(c) avaliação de riscos.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

L

LOG OU REGISTRO DE AUDITORIA: Registro de eventos relevantes em um dispositivo ou sistema computacional.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

M

METADADOS: dados que descrevem os dados, isto é, são informações úteis para identificar, localizar, compreender e gerenciar os dados.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

MODELO DE IMPLEMENTAÇÃO DE NUVEM COMUNITÁRIA: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura da nuvem é compartilhada entre diversas organizações que possuem necessidades comuns, tais como, missão, valores, requisitos de segurança, políticas, requisitos legais, entre outras.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

MODELO DE IMPLEMENTAÇÃO DE NUVEM PRÓPRIA: solução compartilhada de recursos computacionais configuráveis cuja infraestrutura da nuvem pertence apenas a uma organização e suas subsidiárias.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

MUDANÇA: transição ou alteração de uma situação atual.
http://dsic.planalto.gov.br/documentos/nc_13_mudancas.pdf

N

NECESSIDADE DE CONHECER: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

P

PADRÕES CORPORATIVOS DE SISTEMAS E DE CONTROLE: conjunto de regras e procedimentos que compõem os normativos internos das corporações.
http://dsic.planalto.gov.br/documentos/nc_12_dispositivos.pdf

PERFIL DE ACESSO: conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

PERFIL INSTITUCIONAL: cadastro de órgão ou entidade da APF como usuário em redes sociais, alinhado ao planejamento estratégico e à Política de Segurança da Informação e Comunicações (POSIC) da instituição, com observância de sua correlata atribuição e competência.
http://dsic.planalto.gov.br/documentos/nc_15_redes_sociais.pdf

PLANO DE CONTINUIDADE DE NEGÓCIO: 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.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

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.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E COMUNICAÇÕES (POSIC): documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.
http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

PLANO DE RECUPERAÇÃO DE NEGÓCIOS: documentação dos procedimentos e informações necessárias para que o órgão ou entidade da APF operacionalize o retorno das atividades críticas a normalidade.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

PRESERVAÇÃO DE EVIDÊNCIA DE INCIDENTES EM REDES COMPUTACIONAIS: é o processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

PRESTADOR DE SERVIÇO: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

PROGRAMA DE GESTÃO DA CONTINUIDADE DE NEGÓCIOS: processo contínuo de gestão e governança suportado pela alta direção e que recebe recursos apropriados para garantir que os passos necessários estão sendo tomados de forma a identificar o impacto de perdas em potencial, manter estratégias e planos de recuperação viáveis e garantir a continuidade de fornecimento de produtos e serviços por intermédio análises críticas, testes, treinamentos e manutenção.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

PROPRIEDADE DO ATIVO DE INFORMAÇÃO: refere-se a parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação, assumindo, no mínimo, as seguintes atividades:

a) descrever o ativo de informação;

b) definir as exigências de segurança da informação e comunicações do ativo de informação;

c) comunicar as exigências de segurança da informação e comunicações do ativo de informação a todos os custodiantes e usuários;

d) buscar assegurar-se de que as exigências de segurança da informação e comunicações estejam cumpridas por meio de monitoramento; e

e) indicar os riscos que podem afetar os ativos de informação.

http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

Q

QUEBRA DE SEGURANÇA: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

http://dsic.planalto.gov.br/documentos/nc_3_psic.pdf

R

RECURSO CRIPTOGRÁFICO: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração.
http://dsic.planalto.gov.br/documentos/nc_09_revisao_02.pdf

REDES SOCIAIS: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.
https://dsic.planalto.gov.br/documentos/nc_15_redes_sociais.pdf

REQUISITOS DE SEGURANÇA: conjunto de necessidades de segurança que o software deve atender, sendo tais necessidades influenciadas fortemente pela política de segurança da organização, compreendendo aspectos funcionais e não funcionais. Os aspectos funcionais descrevem comportamentos que viabilizam a criação ou a manutenção da segurança e, geralmente, podem ser testados diretamente. Na maioria dos casos, remetem a mecanismos de segurança como, por exemplo, controle de acesso baseado em papéis de usuários (administradores, usuários comuns, etc.), autenticação com o uso de credenciais (usuário e senha, certificados digitais, etc.), dentre outros. Os aspectos não funcionais descrevem procedimentos necessários para que o software permaneça executando suas funções adequadamente mesmo quando sob uso indevido. São exemplos de requisitos não funcionais, dentre outros, a validação das entradas de dados e o registro de logs de auditoria com informações suficientes para análise forense.
http://dsic.planalto.gov.br/documentos/nc_16_software_seguro.pdf

REDUZIR RISCOS: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, adotando ações para reduzir a probabilidade, as consequências negativas, ou ambas, associadas a um risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

RESILIÊNCIA: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

RESUMO CRIPTOGRÁFICO: é um método criptográfico que, quando aplicado sobre uma informação, independente do tamanho desta, gera um resultado único e de tamanho fixo, também chamado de *"hash"*.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

RETER RISCOS: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

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.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

S

SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.
http://dsic.planalto.gov.br/documentos/in_01_gsidsic.pdf

SERVIÇO: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

SISTEMA DE PROTEÇÃO FÍSICA: sistema composto por pessoas, equipamentos e procedimentos para a proteção de ativos contra danos, roubo, sabotagem e outros prejuízos causados por ações humanas não autorizadas, conforme gestão da segurança física e ambiental.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

SISTEMA ESTRUTURANTE: sistema com suporte de tecnologia da informação fundamental e imprescindível para planejamento, coordenação, execução, descentralização, delegação de competência, controle ou auditoria das ações do Estado, além de outras atividades auxiliares, desde que comum a dois ou mais órgãos da Administração e que necessitem de coordenação central.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

T

TEMPO OBJETIVO DE RECUPERAÇÃO: é o tempo pré-definido no qual uma atividade deverá estar disponível após uma interrupção ou incidente.
http://dsic.planalto.gov.br/documentos/nc_6_gcn.pdf

TERMO DE RESPONSABILIDADE: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

TRANSFERIR RISCO: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

TRATAMENTO DA INFORMAÇÃO: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.
http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf

TRATAMENTO DA INFORMAÇÃO CLASSIFICADA: conjunto de ações referentes a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle de informação classificada em qualquer grau de sigilo.
http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf

TRATAMENTO DOS RISCOS: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.
http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf

TRILHA DE AUDITORIA: registro ou conjunto de registros gravados em arquivos de log ou outro tipo de documento ou mídia, que possam indicar, de forma cronológica e inequívoca, o autor e a ação realizada em determinada operação, procedimento ou evento.
http://dsic.planalto.gov.br/documentos/nc_19_SISTEMAS_ESTRUTURANTES.pdf

U

USUÁRIO: servidores, terceirizados, colaboradores, consultores, auditores e estagiários que obtiveram autorização do responsável pela área interessada para acesso aos Ativos de Informação de um órgão ou entidade da APF, formalizada por meio da assinatura do Termo de Responsabilidade.
http://dsic.planalto.gov.br/documentos/nc_07_revisao_01.pdf

USUÁRIO VISITANTE COM DISPOSITIVOS MÓVEIS: agentes públicos ou não que utilizam dispositivos móveis de sua propriedade, ou do órgão ou entidade a que pertencem, dentro dos ambientes físicos e virtuais de órgãos ou entidades da APF, dos quais não fazem parte.
http://dsic.planalto.gov.br/documentos/nc_12_dispositivos.pdf

V

VALOR DO ATIVO DE INFORMAÇÃO: valor, tangível e intangível, que reflete tanto a importância do ativo de informação para o alcance dos objetivos estratégicos de um órgão

ou entidade da APF, quanto o quão cada ativo de informação é imprescindível aos interesses da sociedade e do Estado.
http://dsic.planalto.gov.br/documentos/nc_10_ativos.pdf

VERIFICAÇÃO DE CONFORMIDADE EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES: procedimentos que fazem parte da avaliação de conformidade que visam identificar o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação e comunicações da organização. http://dsic.planalto.gov.br/documentos/nc_11_conformidade.pdf

VULNERABILIDADE: 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.
http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf

ANEXO I

ICP-BRASIL: Certificado 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 Raiz 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. É também a entidade de auditoria de tempo da Rede de Carimbo do Tempo da ICP-Brasil.

A AC-Raiz está encarregada de emitir a lista de certificados revogados, de fiscalizar e auditar as Autoridades Certificadoras (ACs), as autoridades de registros 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.

Conceitos Gerais

Alguns conceitos utilizados na ICP-Brasil são apresentados nesta seção, porém definições adicionais encontram-se em Glossário específico no endereço: *<http://www.iti.gov.br/images/icp-brasil/Normas%20ICP-Brasil/Glossario/GLOSSaRIOV1.4.pdf>*

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.

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.

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.

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. Na estrutura de carimbo de tempo da ICP-Brasil, emite os certificados digitais usados nos equipamentos e sistemas das ACTs e da EAT.

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.

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.

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.

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.

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 como as realizações 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. 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. Cabe informar que a legislação vigente pode ser consultada no sítio do ITI no endereço: <*http://www.iti.gov.br/legislacao*>.

NOTAS SOBRE ESTA EDIÇÃO

Visite <*https://dsic.planalto.gov.br/*> para obter atualizações e outras informações sobre o Guia Básico de Orientações ao Gestor em SIC.

Este trabalho foi produzido no âmbito do Comitê Gestor da Segurança da Informação (CGSI), órgão de assessoramento da Secretaria Executiva do Conselho de Defesa Nacional a qual se subordina - Decreto nº 3.505, de 13 de junho de 2000, e em atendimento à Portaria Nº 26 do Conselho de Defesa Nacional (CDN), de 15 de Julho de 2014, que instituiu o Grupo de Trabalho Elaboração de Guia de Orientações ao Gestor de SIC.