MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES AGÊNCIA ESPACIAL BRASILEIRA	Número da Norma Complementar à POSIC/AEB	Revisão	Emissão	Folha
	03/GTPOSIC /AEB	-	-	01/09
GESTÃO DE RISCO DA AEB				

ORIGEM

Grupo de Trabalho da Política de Segurança da Informação e Comunicações da AEB

REFERÊNCIA NORMATIVA

- Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 01 IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações.
- Norma NBR/ISO/IEC 27.005:2011, que estabelece diretrizes para o gerenciamento dos riscos de Segurança da Informação-SI.
- Norma Complementar nº 08/IN01/CSIC/GSIPR, que estabelece diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.
- Norma Complementar nº 07/IN01/CSIC/GSIPR, que estabelece diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.
- Portaria nº 62/AEB, de 09 de maio de 2017, que estabelece a Política de Gestão de Riscos e Controles Internos da Gestão da AEB

CAMPO DE APLICAÇÃO

Esta Norma se aplica no âmbito da Agência Espacial Brasileira - AEB

SUMÁRIO

APROVAÇÃO
JOSÉ RAIMUNDO BRAGA COELHO
Presidente da Agência Espacial Brasileira

1. OBJETIVO

Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC, da Agência Espacial Brasileira – AEB.

2. CONSIDERAÇÕES INICIAIS

2.1 A implantação do processo de GRSIC busca identificar continuamente as necessidades da AEB em relação aos requisitos de segurança da informação e comunicações, bem como criar e manter atualizado um Sistema de Gestão de Segurança da Informação (SGSI) eficaz.

2.2 A GRSIC, objeto desta norma complementar, está limitada ao escopo das ações de Segurança da Informação e Comunicações
2.3 ,e tais ações compreendem apenas as medidas de proteção dos ativos de informação, conforme elencado na Norma Complementar nº 04/IN01/DSIC/GSI/PR.

2.4 A GRSIC tem como objetivo evitar a ocorrência dos riscos ou minimizar seus efeitos, auxiliando na tomada de decisão, com vistas a prover razoável segurança no cumprimento da missão e no alcance dos objetivos institucionais da AEB.

2.5 Constituem princípios da GRSIC da AEB:

- Considerar riscos e também oportunidades;
- Aplicar-se a qualquer tipo de atividade ou projeto que tenha como escopo a Segurança da Informação e Comunicações;
- Aplicar-se de forma contínua e integrada aos processos de trabalho;
- Ser implantada por meio de ciclos de revisão e melhoria contínua;
- Considerar a importância dos fatores humanos e culturais; e
- Ser dirigida, apoiada e monitorada pela alta administração.

2.6 O processo de gestão de riscos na AEB contempla o estabelecimento do contexto, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e consulta com partes interessadas, o monitoramento e a melhoria contínua.

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

Agente público: todo aquele que exerce cargo, emprego ou função na AEB, ainda que transitoriamente ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745/1993 e empregados públicos regidos pela Lei nº 9.962/2000, e colaboradores).

Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (Ref.: NC 04/IN01/DSIC/GSIPR/2013).

Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco.

Ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento,

transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso (Ref.: NC04/IN01/DSIC/GSIPR/2013).

Avaliação de riscos: processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.

Autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema (Ref.: Lei nº 12.527/2011).

Comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas.

Estimativa de riscos: processo utilizado para atribuir valores à probabilidade e consequências de um risco.

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.

Gestão de Riscos de Segurança da 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.

Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco.

Reduzir risco: 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.

Reter risco: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, assumindo as responsabilidades caso ocorra o risco identificado.

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.

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.

Tratamento dos riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco.

Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização e podem ser evitados por uma ação interna de segurança da informação (Ref.: NC 04/IN01/DSIC/GSIPR/2013).

4. Diretrizes Gerais

I. As diretrizes gerais do processo de GRSIC consideram, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura da AEB, além de estarem alinhadas à POSIC e à POLIGRI da AEB;

II. As decisões estratégicas de Segurança da Informação e Comunicações da AEB devem observar os níveis de exposição aos riscos;

III. Na AEB, será adotada a abordagem sistemática do processo de GRSIC, conforme preconizado na Norma Complementar 04/IN01/DSIC/GSI/PR e na Norma ABNT NBR ISO/IEC 27005:2011, com o objetivo de manter os riscos em níveis aceitáveis;

IV. O processo de GRSIC da AEB deverá ser definido pelas atividades de:

- **a.** Análise de contexto e identificação de requisitos de SIC;
- **b.** Análise e avaliação dos riscos;
- **c.** Definição do plano de tratamento dos riscos;
- **d.** Definição da estratégia de aceitação dos riscos;
- **e.** Implementação do plano de tratamento dos riscos, monitoração e análise crítica;
- **f.** Melhoria do processo de GRSIC;

V. O processo de GRSIC deve ser contínuo e deve estar alinhado ao modelo denominado PDCA (*Plan-Do-Check-Act*), conforme definido na Norma Complementar nº 02/IN01/DSIC/GSIPR, de modo a fomentar a sua melhoria contínua;

VI. O processo de GRSIC deve ser aplicado na implementação e operação da GSI da AEB e deverá produzir subsídios para suportar o Sistema de Segurança da Informação e Comunicações e a Gestão de Continuidade de Negócios da AEB;

VII. Na medida do possível, os riscos de segurança da informação e comunicações devem ser identificados e tratados;

VIII. Todos os usuários devem ficar atentos para identificação e mitigação dos riscos de suas atividades;

IX. A AEB deve difundir uma cultura de identificação e mitigação de risco, na qual procedimentos e sistemas de controle sejam disseminados em todas as áreas administrativas e operacionais, com total comprometimento da Alta Administração da AEB;

X. Um sistema amplo de divulgação, relativo a identificação e mitigação de riscos, deve permear a AEB de forma clara e objetiva;

XI. Uma análise bem estruturada que avalie, identifique e reconheça o comprometimento de todos os usuários com o gerenciamento de riscos de segurança da informação e comunicações é fundamental para o sucesso dessa iniciativa;

XII. A adoção de uma linguagem padrão de GRSIC é essencial ao processo, possibilitando melhor entendimento entre a partes e um processo livre de interferência.

4.1 Valoração dos Ativos

Para efeitos desta Norma Complementar, os ativos da AEB serão categorizados em tangíveis e intangíveis. Os ativos da AEB devem ter seu valor estabelecido, quando necessário, para a confecção dos relatórios guiados por esta Norma Complementar. A valoração dos ativos tangíveis dar-se-á através do valor financeiro consultado no portal de depreciação do Governo Federal. Já para os ativos intangíveis, o valor será atribuído com base no grau de classificação da informação. Quanto mais restrito o acesso àquela informação, maior será o seu valor.

4.2 Avaliação do Impacto

A avaliação do impacto está relacionada à medida do sucesso do incidente. Foi levado em consideração que o impacto tem um efeito imediato ou uma consequência futura, a qual inclui aspectos financeiros e/ou de imagem.

1. Impacto imediato

- **a.** Valor financeiro de reposição do ativo perdido (ou parte dele);
- **b.** O custo de aquisição, configuração e instalação do novo ativo ou do *backup*;

c. O custo das operações suspensas devido ao incidente até que o serviço prestado pelos ativos afetados seja restaurado; e
d. Consequências resultantes de violações da segurança da informação.

2. Impacto Indireto
a. Custo de oportunidade (recursos financeiros necessários para repor ou reparar um ativo poderiam estar sendo utilizados para outro fim);
b. O custo das operações interrompidas;
c. Mau uso das informações obtidas através da violação da segurança;
d. Violação de obrigações estatutárias ou regulatórias; e
e. Violação dos códigos éticos de conduta.

4.3 Ameaças Comuns

A tabela a seguir serve de apoio para o processo de avaliação das ameaças. As ameaças podem ser intencionais, acidentais ou de origem ambiental e podem resultar, por exemplo, no comprometimento ou na paralisação de serviços essenciais. A letra na coluna de origem indica o tipo de ameaça, sendo A (acidental), I (intencional) e N (natural).

Tabela 1-Ameaças Comuns

Tipo	Ameaças	Origem
Dano Físico	Fogo	A,I,N
	Água	A,I,N
	Poluição	A,I,N
	Acidente grave	A,I,N
	Destruição de equipamento ou mídia	A,I,N
	Poeira, corrosão, falha no sistema de refrigeração	A,I,N
Eventos naturais	Fenômeno climático	N
	Fenômeno sísmico	N
	Fenômeno meteorológico	N
	Inundação	N
Paralisação de serviços essenciais	Falha do ar condicionado no datacenter ou do sistema de suprimento de água	A,I
	Interrupção do suprimento de energia	A,I,N
	Falha do equipamento de telecomunicação	A,I
Distúrbio causado por radiação	Radiação eletromagnética	A,I,N
	Radiação térmica	A,I,N
	Pulsos eletromagnéticos	A,I,N
Comprometimento da informação	Interceptação de sinais de interferência comprometedores	I
	Espionagem	I
	Escuta não autorizada	I
	Furto de mídia ou documentos	I
	Furto de equipamentos	I
	Recuperação de mídia reciclada ou descartada	I
	Divulgação indevida	A,I
	Dados de fontes não confiáveis	A,I

	Alteração do hardware	I
	Alteração de software	A,I
	Determinação da localização	I
Falhas técnicas	Falha de equipamento	A
	Defeito de equipamento	A
	Saturação do sistema de informação	A,I
	Defeito de *software*	A
	Violação das condições de uso do sistema de informação que possibilitem sua manutenção	A,I
Ações não autorizadas	Uso não autorizado de equipamento	I
	Cópia ilegal de *software*	I
	Uso de cópias de *software* falsificadas ou ilegais	A,I
	Comprometimento dos dados	I
	Processamento ilegal de dados	I
Comprometimento de funções	Erro durante o uso	A
	Abuso de direitos	A,I
	Forjamento de direitos	I
	Repúdio de ações	I
	Indisponibilidade de recursos humanos	A,I,N

4.4 Avaliação de Riscos de Segurança da Informação

O processo de avaliação de risco de segurança da informação envolve a identificação e valoração dos ativos, suas ameaças e vulnerabilidades. O objetivo da atividade é usar essa informação para identificar o tratamento do risco.
Para cada risco identificado, é necessário analisar a probabilidade e o impacto de ocorrência, sendo aplicado uma escala com 5 níveis de classificação: muito baixo, baixo, médio e alto e muito alto. Os critérios adotados para realizar a classificação estão descritos abaixo:

Tabela 2-Grau de Probabilidade

Grau de probabilidade	Definição
Muito Baixo	Estima-se uma probabilidade quase improvável desse evento ocorrer
Baixo	Estima-se uma menor probabilidade desse evento ocorrer
Médio	Estima-se uma média probabilidade desse evento ocorrer
Alto	Estima-se uma alta probabilidade desse evento ocorrer
Muito Alto	Estima-se que esse evento ocorrerá em um futuro próximo

Tabela 3-Grau de Impacto

Grau de impacto	Definição/Efeitos
Muito Baixo	• Os efeitos do evento são quase imperceptíveis; • Na maioria das vezes, o custo da prevenção do evento é maior que o custo dos efeitos do evento; quando esses eventos afetam o custo, o prazo ou a qualidade do projeto ou atividade podem ser facilmente reparados e ajustados, não causando ameaças ao sucesso do projeto.
Baixo	• Baixo impacto para algumas atividades; • Frequentemente este item significa alguma fraqueza de controle.
Médio	• Os efeitos são moderados; • Quando esses eventos afetam o custo, o prazo ou a qualidade do projeto ou atividade, podem ser reparados e ajustados, entretanto os impactos podem afetar o plano do projeto, necessitando de repactuação de prazos e custos.
Alto	• Os efeitos do evento são elevados; • Quando esses eventos afetam o custo, o prazo ou a qualidade do projeto ou atividade, somente podem ser reparados através de replanejamento, necessitando de renegociação de prazos e custos entre as partes.
Muito Alto	• Impacto catastrófico às operações: estratégicas, financeiras, programas, captação de recursos e aquisições; • Impede a continuação normal da atividade; • Perda de confiança por parte dos parceiros do projeto; • Sanções regulatórias graves; • Questões que requerem atenção do Comitê de Tecnologia da Informação, instituído pela portaria nº 97 AEB, de 14 de maio de 2017.

A matriz abaixo representa, em escala de cores, o grau do risco baseado na Probabilidade x Risco.

Tabela 4-Escala de Cores (Probabilidade x Risco)

Classificação dos Riscos		Probabilidade				
		Muito Baixa	Baixa	Média	Alta	Muito Alta
Impacto	Muito baixo	1	2	3	4	5
	Baixo	2	4	6	8	10
	Médio	3	6	9	12	15
	Alto	4	8	12	16	20
	Muito Alto	5	10	15	20	25

Para o cálculo do grau de criticidade de cada risco, elencado na Tabela 4 – Escala de Cores, foram utilizadas as seguintes pontuações, tanto para a probabilidade quanto para o impacto: quando o risco for

classificado como muito baixo, será adotada a pontuação 1; quando for classificado como baixo, será adotada a pontuação 2; quando for classificado como médio, será adotada a pontuação 3; quando o risco for classificado como alto, será adotada a pontuação 4 e; quando o for classificado como muito alto, será adotada a pontuação 5. O cálculo do grau de criticidade será dado pela multiplicação entre probabilidade e impacto.

A pontuação descrida em cada item será considerada para estipular a priorização no plano de tratamento do risco, fazendo um *rankeamento* e, baseada nessa pontuação, serão propostas ações para mitigar aquele risco. Essas ações estarão descritas na coluna de contramedidas de uma tabela de riscos e servirão como base para a criação do Plano de Continuidade.

Caso existam riscos com a mesma pontuação, o critério adotado de desempate, para efeito desta norma, considerar-se-á o valor mais alto na seguinte ordem:

- **1º:** Grau de impacto do risco;
- **2º:** Grau de probabilidade do risco;
- **3º:** Grau de classificação das informações influenciadas pelo risco, adotando sempre o maior;
- **4º:** Valor financeiro do ativo envolvido no risco.

5. VIGÊNCIA

Esta Norma Entra em vigor na data de sua publicação.