PORTARIA CNMP-PRESI Nº 167, DE 4 DE DEZEMBRO DE 2018.

Versão Compilada

Vide Portaria CNMP-PRESI nº 214, de 2 de dezembro de 2019

Institui o Plano de Gestão de Riscos e o Plano de Segurança Institucional do Conselho Nacional do Ministério Público.

A PRESIDENTE DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO, no uso das atribuições que lhe conferem o art. 130-A, § 2º, I, da Constituição Federal e o art. 12, I, XII, XIII, XVII, XXVI e XXVII, do Regimento Interno do Conselho Nacional do Ministério Público e tendo em vista o que consta do Procedimento Administrativo nº 19.00.5000.0006202/2017-75, RESOLVE:

Considerando o disposto na Portaria CNMP-PRESI nº 45, de 27 de abril de 2017, que institui a Política de Gestão de Riscos do Conselho Nacional do Ministério Público; e

Considerando o disposto na Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017, que regulamenta a Política de Segurança Institucional do Conselho Nacional do Ministério Público, RESOLVE:

Art. 1º Publicar o Plano de Gestão de Riscos do Conselho Nacional do Ministério Público, constante do anexo I desta Portaria.

Art. 2º Publicar o Plano de Segurança Institucional do Conselho Nacional do Ministério Público, constante do anexo II desta Portaria.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

Brasília-DF, 4 de dezembro de 2018.

RAQUEL ELIAS FERREIRA DODGE

ANEXO I

PORTARIA CNMP-PRESI Nº 167, DE 30 DE NOVEMBRO DE 2018.

PLANO DE GESTÃO DE RISCOS DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

1. INTRODUÇÃO

No dia 1º de março de 2016, o Comitê de Governança Corporativa e da Estratégia (CGCE), em reunião ordinária, aprovou a criação de Grupo de Trabalho para estudar e propor a Cadeia de Valor e as políticas de gestão de riscos e de segurança institucional do CNMP (GT-Riscos), em atendimento ao Acordão nº 1273/2015-TCU-Plenário e ao disposto no art. 27 da Portaria CNMP-PRESI nº 36, de abril de 2016, revogada pela Portaria CNMP-PRESI nº 25, de fevereiro de 2018. Ao final de dezesseis encontros com profícuos debates sobre o tema, o Grupo concluiu três produtos: a Cadeia de Valor do CNMP (Portaria CNMP-PRESI nº 37, de 18 de abril de 2017); a Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45, de 27 de abril de 2017); a Política de Segurança Institucional (Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017).

A Cadeia de Valor do CNMP consiste na representação gráfica dos principais macroprocessos que agregam valor à instituição, alinhada à possibilidade de análise das relações entre eles e como cada um deles contribui para o cumprimento das atribuições do órgão. Já as Políticas de Gestão de Riscos e de Segurança Institucional estabelecem objetivos, princípios, diretrizes, recursos, responsabilidades e procedimentos em conformidade com as melhores práticas adotadas pelo setor público, alinhados com o Planejamento Estratégico e a Cadeia de Valor do CNMP.

Essas iniciativas têm por objetivo minimizar os riscos das principais atividades aqui desenvolvidas e aumentar a segurança da instituição em sua atuação, tendo por consequência maior eficiência na prestação de serviços para a sociedade.

Este documento detalhará o processo de gestão de riscos previsto na Política de Gestão de Riscos do CNMP, servindo de referência para todas as unidades do CNMP, sem prejuízo da utilização de outras normas complementares específicas relativas à Instituição ou suas unidades.

Para a elaboração deste documento, foram utilizados planos e manuais de referência, quais sejam, *Enterprise Risk Management – Integrated Framework* (COSO II) e a norma ABNT NBR ISO 31000. Além disso, foi feito *benchmarking* nas seguintes instituições: Tribunal de Contas da União, Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Transparência e Corregedoria Geral da União, Tribunal Superior do Trabalho, Tribunal Regional do Trabalho da 18ª Região e Tribunal Regional Eleitoral do Rio Grande do Sul.

2. TERMOS E DEFINIÇÕES

Para fins deste documento, consideram-se os seguintes conceitos:

• Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e, na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.

• Objeto de avaliação de riscos: ações, projetos, iniciativas, ativos e processos de trabalho que são executados para alcançar produto, resultado ou serviço prestado.

~~• Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.~~

~~• Gestor de riscos: pessoa ou entidade com responsabilidade e autoridade para gerenciar um risco.~~

~~• Controle interno: conjunto de atividades, planos, métodos, indicadores e procedimentos interligados, estabelecidos com vistas a assegurar que os diversos objetivos das unidades do CNMP sejam alcançados, evidenciando eventuais desvios.~~

~~• Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos.~~

~~• Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos.~~

~~• Eventos de risco: incidente ou uma ocorrência que afeta a realização dos diversos objetivos do CNMP.~~

~~• Consequências: resultado de um evento que afeta os diversos objetivos do CNMP.~~

~~• Causas: condições que viabilizam a concretização de um evento que afetam os objetivos. São resultantes da junção das fontes de risco com as vulnerabilidades.~~

~~• Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.~~

~~• Vulnerabilidades: Ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.~~

~~• Nível de risco: magnitude de um risco, expressa em termos da combinação das probabilidades e do impacto.~~

~~• Risco: possibilidade que um evento, iminente ou futuro, ocorra e afete negativamente a realização dos objetivos do CNMP.~~

~~• Risco inerente: risco ao qual ações, projetos, iniciativas, ativos e processos de trabalho do CNMP estão sujeitos, desconsiderados os controles existentes.~~

~~• Risco residual: risco remanescente após a incidência dos controles aplicados.~~

~~• Risco emergente: risco decorrente da adoção das medidas de controle para um risco inerente ou residual.~~

~~• Critérios de risco: padrão de referência para a avaliação dos riscos.~~

~~• Apetite a risco: nível de risco que o CNMP se dispõe a aceitar na busca por agregar valor aos serviços prestados.~~

~~• Análise de riscos: processo de compreender a natureza do risco e determinar o nível de risco.~~

~~• Avaliação de riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.~~

~~• Tratamento de riscos: abordagem do CNMP após avaliar o risco e, a partir daí, adotar medidas para evitá-lo, transferi-lo/compartilhá-lo, mitigá-lo e, eventualmente, aceitá-lo.~~

~~• Medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.~~

~~• Matriz RACI: corresponde à sigla para *Responsible*, *Accountable*, *Consulted* e *Informed* (em português, pode-se traduzir livremente para Responsável, Aprovador, Consultado e Informado). Assim, a matriz RACI é uma ferramenta por meio da qual cada colaborador toma consciência de suas atribuições durante o processo de gestão de riscos. É uma matriz de distribuição de responsabilidades.~~

3. ESTRUTURA DE GESTÃO DE RICOS DO CNMP

Segundo a norma ISO 31000 (norma da família de gestão de risco criada pela International Organization for Standardization, cujo objetivo é estabelecer princípios e orientações genéricas sobre gestão de riscos nas organizações), a gestão de riscos em uma organização possui três pilares: os princípios, a estrutura e o processo.

No âmbito do CNMP, nos termos dos art. 3º e 4º da Portaria CNMP-PRESI nº 45, de 27 de abril de 2017, que institui a Política de Gestão de Riscos do CNMP, os princípios foram desdobrados em diretrizes e objetivos, respectivamente, conforme quadro abaixo:

Quadro 1 – Diretrizes da Gestão de Riscos do CNMP

Princípios da Gestão de Riscos no CNMP	Diretrizes	• Conformidade dos processos à legislação aplicável • Alinhamento ao Planejamento Estratégico e à Cadeia de Valor • Promoção dos valores institucionais • Disseminação da cultura de gestão de riscos • Adequação do apetite ao risco às estratégias adotadas • Comprometimento das partes envolvidas nos processos organizacionais de tomada de decisões • Dinamismo, iteratividade e capacidade de reagir a mudanças • Fomento à melhoria contínua da gestão
	Objetivos	• Identificar potenciais eventos que afetem o alcance da missão institucional • Fornecer informações íntegras para o processo de tomada de decisão • Aprimorar os processos de controle interno

Em relação à estrutura de gestão de riscos, a referida ISO conceitua que é o "*conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização*". Ainda dentro da estrutura, a norma mencionada trata dos seguintes componentes: Mandato e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura.

No CNMP, o componente Mandato e Comprometimento é demonstrado pelas ações do Comitê de Governança Corporativa e da Estratégia (CGCE), do Subcomitê de Gestão de Riscos e Segurança Institucional (SERSI) e da alta administração em promover a Gestão de Riscos do CNMP.

Na Concepção da Estrutura para Gerenciar Riscos, além do CGCE e do SERSI, foi definida a Política de Gestão de Riscos por meio da Portaria CNMP-PRESI nº 45/2017 e foi instituído o SERSI pela Portaria CNMP-PRESI nº 50/2018, normativos que definem o processo de gestão de riscos e as competências e responsabilidades.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos do CNMP, é prevista revisão da Política de Gestão de Riscos e deste Plano em período não superior a dois anos (Melhoria Contínua da Estrutura). Porém, mudanças no contexto do CNMP podem provocar a necessidade de implantação de melhorias de forma antecipada, desde que propostas pelo SERSI e aprovadas pela Secretaria-Geral do CNMP, conforme inciso III do art. 10-E da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018, que altera a Portaria CNMP-PRESI nº 160/2014, instituindo o SERSI no âmbito do CGCE.

3.1 Das Competências

As competências quanto à gestão de riscos do CNMP foram definidas na Política de Gestão de Riscos, na Portaria que institui o SERSI, bem como neste documento. Desse modo, a governança de gestão de riscos configura-se em três níveis:

- nível estratégico com o Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI);
- nível tático com a Secretária de Gestão Estratégica (SGE); e
- nível operacional com o gestor de riscos.

Outrossim, compete à Secretaria-Geral presidir o SERSI, realizar estudos e adotar as medidas necessárias para a edição, pela Presidência, de atos normativos dispondo sobre a gestão do conhecimento e a implementação da gestão de riscos e segurança institucional, nos termos do art. 27 da Portaria CNMP-PRESI nº 25, de 22 de fevereiro de 2018, que dispõe sobre o PE-CNMP.

3.1.1 Do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional

A principal instância de governança sobre gestão de riscos do CNMP é o SERSI, instituído por meio da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018. Vinculado ao CGCE, o Subcomitê Estratégico é composto por representantes das seguintes unidades: Presidência; Corregedoria Nacional; Secretaria-Geral; Comissões; Secretaria de Gestão Estratégica; Secretaria de Administração; Secretaria Processual; Secretaria de Tecnologia da Informação; Assessoria de Comunicação Social; Auditoria Interna; Coordenadoria Gestão de Pessoas e Coordenadoria de Segurança e Transporte.

As competências do SERSI estão definidas no art. 10-E da Portaria CNMP-PRESI nº 160/2014, quais sejam:

- analisar e deliberar sobre riscos ou ameaças que possam comprometer a prestação de serviços, a imagem junto à sociedade, a autonomia e a efetividade dos resultados no alcance da estratégia;
- monitorar, avaliar e propor a revisão das Políticas de Gestão de Riscos e de Segurança Institucional, periodicamente, submetendo-as à apreciação da Presidência do CNMP;
- elaborar, monitorar, avaliar e propor a revisão do Plano de Gestão de Riscos e do Plano de Segurança Institucional, submetendo-os à deliberação da Secretaria-Geral;
- definir, anualmente, o apetite a riscos do CNMP, conforme previsto na Política de Gestão de Riscos do CNMP; e
- avaliar a eficácia e a efetividade do processo de gerenciamento de riscos e da segurança institucional.

3.1.2 Da Secretaria de Gestão Estratégica

Segundo o §5º do art. 10-E da Portaria CNMP-PRESI nº 160/2014, a coordenação do processo de gestão riscos do CNMP compete à Secretaria de Gestão Estratégica (SGE). Desse modo, especificam-se as seguintes competências:

- auxiliar o SERSI na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de

gerenciamento de riscos;

• monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;

• dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;

• consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento;

• oferecer capacitação continuada em Gestão de Riscos para os servidores do CNMP;

• promover a disseminação da cultura de gestão de riscos; e

• requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

3.1.3 Do gestor de riscos

A Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45/2017) define as seguintes competências aos gestores de riscos, relativamente aos objetos de avaliação de riscos sob sua responsabilidade:

• escolher, justificadamente, dentre os objetos (ações, projetos, iniciativas, ativos e processos de trabalho) sob sua responsabilidade, quais terão os riscos gerenciados, à vista da dimensão dos prejuízos que possam causar;

• assegurar que o risco seja gerenciado de acordo com os critérios do processo de gestão de riscos estabelecidos neste Plano; e

• gerar e reportar informações adequadas sobre a gestão de riscos às instâncias de governança.

Ainda, de acordo com o art. 15 da Portaria CNMP-PRESI nº 45/2017, são considerados **gestores de riscos**, dentre outros, o Presidente, o Corregedor Nacional, o Ouvidor Nacional, os Conselheiros, os presidentes e membros auxiliares das comissões permanentes e temporárias, o Secretário-Geral, os secretários e titulares de unidades administrativas.

4. PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos no CNMP dar-se-á sobre ações, projetos, iniciativas, ativos e processos de trabalho. Quanto aos processos de trabalho, serão levados em consideração os constantes do 3º nível da Cadeia de Valor. Cabe aos gestores de risco, conforme as responsabilidades definidas na Política de Gestão de Riscos, escolher os objetos que devam ter os riscos gerenciados e tratados com prioridade em cada unidade do CNMP, em face da dimensão dos prejuízos que a não gestão dos riscos possa causar. Ainda podem ser levados em consideração critérios de escolha, tais como: o alinhamento do processo com os objetivos estratégicos do CNMP e o impacto em caso de incidentes ou o custo do processo.

Definido o objeto, convém ao gestor de riscos elaborar uma matriz RACI, que estabelece as responsabilidades específicas para cada atividade da gestão de riscos em cada unidade. Assim, o responsável (R) é quem efetivamente irá executar a atividade; o aprovador (A) é o responsável pelo aceite formal da atividade ou produto entregue, podendo delegar a função para outros profissionais, mas não a responsabilidade; o consultado (C) é a pessoa que possa fornecer informação sobre a referida atividade; e o informado (I) é a pessoa ou os grupos de pessoas que precisam ser notificados de resultados ou ações tomadas, mas não precisam estar envolvidos no processo de tomada

de decisão. O Quadro 2 apresenta um modelo de matriz de responsabilidades (RACI).

Quadro 2 – Matriz RACI para o processo de gerenciamento de riscos

Atividade	**SG**	**SERSI**	**SGE**	**Gestor de Riscos**	**Servidor**
Estabelecer o contexto	-	-	-	-	-
Identificar os riscos	-	-	-	-	-
Analisar os riscos	-	-	-	-	-
Avaliar os riscos	-	-	-	-	-
Tratar os riscos	-	-	-	-	-
Elaborar o Plano de Tratamento de Riscos	-	-	-	-	-
Monitoramento e análise crítica	-	-	-	-	-
Comunicar e consultar	-	-	-	-	-
Capacitar envolvidos	-	-	-	-	-

***R** – Responsável; **A** – Aprovador; **C** – Consultado; **I** – Informado*

Uma vez definida a priorização, dar-se-á início ao processo de gestão de riscos, conforme modelo da Norma ABNT NBR 31000:2009, adaptada à realidade do CNMP, com as seguintes atividades:

• estabelecimento do contexto;

• identificação e análise de riscos;

• avaliação de riscos;

• tratamento de riscos;

• monitoramento e análise crítica; e

• comunicação e consulta.

As atividades, que interagem de forma cíclica, são definidas a seguir com os principais artefatos e atores envolvidos.

4.1 Estabelecimento do Contexto

Nesta etapa, devem ser identificados, pelo menos:

• descrição resumida do objeto que terá os riscos gerenciados;

• objetivos a serem alcançados pelo objeto;

• relação de objetivos estratégicos do CNMP alcançados pelo objeto; e

• justificativa para a aplicação do processo de gerenciamento de riscos no objeto.

Também é necessária a definição dos parâmetros gerais externos e internos e dos critérios de risco a serem levados em consideração ao gerenciar riscos no CNMP. Essa atividade é de fundamental importância, pois é a partir dela que todas as demais atividades serão desenvolvidas. A fim de deixar o plano mais didático, os critérios de riscos serão definidos ao longo das demais atividades, à medida que forem sendo utilizados.

4.1.1 Parâmetros gerais internos e externos

Em relação aos parâmetros gerais, eles funcionam como guias, direcionadores para a identificação dos riscos. Eles são compostos pelos seguintes fatores, entre outros:

• Parâmetros internos: Conformidade e Fiscalização, Recursos Humanos, Tecnologia da Informação,

Controles Físicos e Cultura Organizacional.

• Parâmetros externos: Ambiente Legal, Fornecedores, Reputação, Econômicos e Ambiente Cultural, Social e Político.

Quadro 3 – Parâmetros gerais internos e externos, fatores e subfatores

PARÂMETROS INTERNOS	**PARÂMETROS EXTERNOS**
Conformidade e Fiscalização • Normatização; • Fiscalização e controle interno; • Outros.	**Ambiente Legal** • Ambiente regulatório; • Aderência aos principais requisitos regulatórios externos; • Outros.
Recursos Humanos • Carga de trabalho; • Segregação de funções; • Clima organizacional; • Outros.	**Fornecedores** • Relação com os fornecedores; • Sanções ao contratado; • Cláusulas contratuais sobre a entrega do objeto contratado; • Outros.
Tecnologia da Informação • Sistemas obsoletos; • Demanda interna por recursos de TI; • Definição de parâmetros mínimos de qualidade e eficiência dos serviços prestados pela TI; • Outros.	**Reputação** • Percepção da sociedade; • Outros.
Controles Físicos • Controles de segurança física; • Alinhamento entre os controles de segurança física e lógica; • Outros.	**Econômicos** • Restrições orçamentárias; • Contingenciamento; • Outros.
Cultura Organizacional • Adaptação da cultura organizacional às mudanças no contexto interno; • Outros.	**Ambiente Cultural, Social e Político** • Mudanças de governo; • Outros.

O gestor de riscos, em conjunto com sua equipe, pode estabelecer seus parâmetros internos e externos específicos. Para tanto, ele tem a possibilidade de ajustar as categorias de parâmetros e subparâmetros, excluindo as que não se aplicam ao objeto de análise e incluindo as que não estejam previstas.

O estabelecimento dos parâmetros gerais é importante por dois motivos básicos: primeiro, no decorrer do tempo, possibilita a Instituição a fazer uma categorização de seus principais riscos; segundo, eles são elementos direcionadores no momento de pensar os riscos das unidades.

4.2 Identificação e análise de riscos

A identificação dos riscos consiste na busca, no reconhecimento e na descrição de riscos, mediante a identificação das fontes de risco, eventos, suas causas e consequências potenciais. A finalidade dessa etapa é gerar uma lista abrangente de eventos que possam evitar, prejudicar, impedir ou atrasar o cumprimento dos objetivos do objeto de avaliação de riscos. A identificação abrangente é fundamental, pois um risco que não é identificado nesta fase não será incluído em análises posteriores.

Nessa fase, o gestor poderá utilizar como referência os parâmetros gerais internos e externos definidos no item 4.1.1. Para a identificação dos riscos, o gestor pode utilizar técnicas como *brainstorming*, entrevista com

especialistas, entre outras. Uma vez identificado o risco, o gestor deverá categorizá-lo como estratégico, operacional, de conformidade ou de reputação. Vale ressaltar que um risco pode ser classificado em mais de uma categoria. Destaca-se que essas categorias de riscos estão definidas nos incisos V a VIII do art. 2º da Portaria CNMP-PRESI nº 45/2017.

Identificados e categorizados os riscos, convém analisá-los de forma criteriosa, pois essa análise fornece subsídios para a avaliação de riscos, bem como para as estratégias, métodos e decisões de tratamento dos riscos. A análise envolve a apreciação das causas e das fontes de riscos, suas consequências negativas e a probabilidade de que esses eventos venham a ocorrer.

Nessa etapa, é importante apontar os fatores que afetam as consequências e a probabilidade de ocorrência dos riscos, ou a combinação de ambos, confrontados com os controles existentes, a fim de testar a eficácia e a eficiência desses controles. A combinação das consequências, as quais podem ser expressas em termos de impactos tangíveis e intangíveis, com a probabilidade, serve para determinar o nível do risco inerente.

O Quadro 4 apresenta o Formulário de Identificação e Análise de Riscos.

Quadro 4 – Formulário de Identificação e Análise de Riscos

Objeto de Avaliação de Riscos:			-		**Copilado por:** **Data:**	
Objetivo:			-		**Analisado por:** **Data:**	
Relação de Objetivos Estratégicos:			-		-	
Justificativa para o gerenciamento:			-		-	
Riscos Identificados						
ID	**Eventos de Risco**	**Causas**	**Consequências**	**Parâmetro Externo**	**Parâmetro Interno**	**Categoria do Risco**
1	-	-	-	-	-	-
2	-	-	-	-	-	-
3	-	-	-	-	-	-

4.3 Avaliação de riscos

A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados das etapas anteriores, sobre quais riscos necessitam de tratamento e a prioridade para a implementação das ações de tratamento do risco.

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios do processo de gestão do CNMP, quais sejam: probabilidade, impacto, apetite a riscos, matriz de classificação de riscos, diretrizes para priorização e tratamento, e matriz da eficácia dos controles.

A probabilidade diz respeito às chances de um evento ocorrer. Dessa forma, o Quadro 5 define os graus de probabilidade e os respectivos níveis.

Quadro 5 – Escala de probabilidade

Descritor	Descrição	Nível
Muito Baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3
Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito Alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, pois as circunstâncias indicam claramente essa possibilidade.	5

Fonte: Adaptado de Plano de Gestão de Riscos (TST, 2015)

O impacto, por sua vez, está relacionado às consequências do evento nos objetos, caso ele ocorra. Visando a diminuir a subjetividade do método, optou-se por definir o nível desse impacto considerando as dimensões custo, prazo, escopo e qualidade do objeto analisado. Desse modo, primeiramente o gestor deve analisar o impacto nessas dimensões, conforme quadro abaixo:

Quadro 6 – Escala de impacto

Impacto nas dimensões do objetivo				
Custo (aumento)	Prazo (atraso)	Escopo (afetação)	Qualidade (degradação)	Nível
Muito Baixo	Insignificante	Insignificante	Irrisória	1
Baixo	Pequeno	Pouca	Pouca	2
Médio	Moderado	Significativa	Relevante	3
Alto	Grande	Muito significativa	Muito relevante	4
Muito Alto	Catastrófico	Ampla	Grave	5

Fonte: Adaptado de Plano de Gestão de Riscos (TST, 2015)

Sobre o Quadro 6, pode ocorrer de os níveis serem diferentes para cada dimensão. Nesse caso, o gestor de riscos deve considerar o nível mais alto. Por exemplo, caso na dimensão Custo o gestor considere que haverá um aumento muito baixo do orçamento (nível 1) e na dimensão Qualidade considere que haverá uma degradação grave (nível 5), o nível a ser considerado será o 5.

Uma vez estabelecidos os níveis dessas dimensões, definem-se os graus do impacto com o respectivo nível, conforme Quadro 7.

Quadro 7 – Graus de impacto

Grau	Descrição	Nível
Muito Baixo	Impacto insignificante nos objetivos.	1
Baixo	Impacto mínimo nos objetivos.	2
Médio	Impacto mediano nos objetivos, com possibilidade de recuperação.	3
Alto	Impacto significante nos objetivos, com possibilidade remota de recuperação.	4
Muito Alto	Impacto máximo nos objetivos, sem possibilidade de recuperação.	5

Fonte: Plano de Gestão de Riscos (TST, 2015)

Tendo em mãos os níveis de probabilidade e impacto, o gestor de riscos deve fazer a multiplicação desses níveis, que define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

O risco pode ser classificado dentro das seguintes faixas:

Quadro 8 – Classificação do risco

Classificação	Faixa
Risco Baixo	0 – 4,99
Risco Médio	5,00 – 9,99
Risco Alto	10,00 – 14,99
Risco Extremo	15,00 – 25,00

Fonte: Adaptado de Gestão de Riscos – Avaliação da Maturidade (TCU, 2018)

Quadro 9 – Matriz de riscos

Nível de Risco Extremo Alto Médio Baixo		PROBABILIDADE				
		Muito baixa 1	Baixa 2	Média 3	Alta 4	Muito alta 5
IMPACTO	Muito alto 5	5	10	15	20	25
	Alto 4	4	8	12	16	20
	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito baixo 1	1	2	3	4	5

Para finalizar os critérios de riscos, o CNMP definiu a Tabela da Eficácia dos Controles Existentes (Quadro 10), a qual estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual. Esse quadro deve ser aplicado logo após a definição dos níveis de riscos, caso já existam controles implementados, e após a adoção das medidas de tratamento dos riscos.

Quadro 10 – Eficácia dos controles existentes

Eficácia do Controle	Situação do controle	Multiplicador do Risco Inerente
Inexistente	Ausência completa de controle.	1,0
Fraco	Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	0,8
Mediano	Controle pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,6
Satisfatório	Controle normatizado e, embora passível de aperfeiçoamento, está sustentado por ferramentas adequadas e mitiga o risco razoavelmente.	0,4
Forte	Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de "melhor prática".	0,2

Fonte: Plano de Gestão de Riscos (TST, 2015)

Ressalta-se, também, que o apetite a risco do CNMP levará em consideração o risco no **nível baixo**, ou seja, para riscos nesse nível, não há a necessidade de ações e medidas de tratamento. Assim, basta apenas o seu monitoramento constante para assegurar que eles ainda se encontram nesses patamares.

O Quadro 11 representa o Formulário de Avaliação de Riscos:

Quadro 11 – Formulário de Avaliação de Riscos

Objeto de Avaliação de Riscos:							**Compilado por:** **Data:**			
Objetivo:							**Analisado por:** **Data:**			
Riscos Identificados				**Probabilidade**	**Impacto**	**Risco Inerente**	**Controles Existentes**			**Risco Residual**
ID	**Eventos de Risco**	**Causas**	**Consequências**				**Descrição**	**Eficácia**		
1	-	-	-	-	-		-	-	-	
							-	-	-	
							-	-	-	
2	-	-	-	-	-		-	-	-	
							-	-	-	
							-	-	-	

4.4 Tratamento de Riscos

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para definir as diretrizes para respostas consoante quadro a seguir:

Quadro 12 – Diretrizes para resposta perante o nível do risco

Nível de Risco	**Descrição**	**Diretriz para Resposta**
Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação pelo Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI).	Qualquer risco encontrado nessa área deve ter uma resposta imediata. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 15 dias. O plano de ação deverá ser apreciado pelo Subcomitê, aprovado pelo Secretário Geral e implementado em até 3 meses. O monitoramento será feito no Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos, apreciação do Subcomitê e aprovação do Secretário Geral.
Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação da Reunião de Acompanhamento Tático (RAT).	Qualquer risco encontrado nessa área deve ter uma resposta em até 15 dias. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 30 dias. O plano de ação deverá ser apreciado na Reunião de Acompanhamento Tático (RAT), aprovado pelo Secretário Geral e implementado em até 6 meses. O monitoramento será feito na Reunião de Acompanhamento Tático (RAT). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos e aprovação do Secretário Geral.
Médio	Nível de risco além do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	O gestor de riscos da unidade deve adotar medidas de tratamento no decorrer de um ano. O monitoramento será feito nas RAOs.
Baixo	Nível de risco dentro do apetite a risco, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades se determinado pelo gestor de riscos.

As ações de tratamento de riscos são: evitar o risco, não iniciando ou descontinuando a atividade que dá origem ao risco; mitigar o risco, implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências; aceitar o risco, assumindo o risco, por escolha consciente e justificada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício; e transferir o risco, compartilhando ou transferindo o risco com outra parte interessada.

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos. A implementação do tratamento pode gerar novos controles ou modificar os controles existentes. A fase inicial do tratamento de riscos é a elaboração do Plano de Tratamento de Riscos, que deve levar em consideração a eficácia das ações já existentes, as restrições organizacionais, técnicas e estruturais, os requisitos legais, a análise custo-benefício e as ações a serem realizadas. Além disso, no Plano de Tratamento de Riscos devem constar os responsáveis, as prioridades e os prazos de execução.

Quadro 13 – Plano de Tratamento de Riscos

Objeto de Avaliação de Riscos:								**Compilado por:** **Data:**		
Objetivo:								**Analisado por:** **Data:**		
Riscos Prioritários				**Categoria do Risco**	**Tipo de Tratamento**	**Ações e Medidas de Tratamento**	**Relação Custo-Benefício**	**Responsável**	**Período de Execução**	**Monitoramento do Risco e seu Tratamento**
ID	**Eventos de Risco**	**Causas**	**Consequências**							
1	-	-	-	-	-	-	-	-	-	-
					-	-	-	-	-	
2	-	-	-	-	-	-	-	-	-	-
					-	-	-	-	-	
3	-	-	-	-	-	-	-	-	-	-
					-	-	-	-	-	

4.5 Monitoramento e Análise Crítica

A fase de monitoramento e análise crítica acontecerá nas reuniões do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional, nas Reuniões de Acompanhamento Tático, nas Reuniões Acompanhamento Operacional e por meio do gestor de riscos, periodicamente ou quando acontecer em resposta a um fato específico.

Entre as finalidades do monitoramento e análise crítica estão a garantia de que os controles sejam eficazes e eficientes, a obtenção de informações adicionais para melhorar a avaliação dos riscos e identificar os riscos residuais que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo.

O Quadro 14 representa o Formulário de Monitoramento e Análise.

Quadro 14 – Formulário de Monitoramento e Análise

Objeto de Avaliação de Riscos: - - - - - - - - - - - -						**Compilado por:** **Data:**						
Objetivo: - - - - - - - - - - - -						**Analisado por:** **Data:**						
Risco				**Categoria do Risco**	**Controles existentes**	**Data**	**Ocorrência do Risco**	**Novos controles**	**Risco Residual**	**Melhoria**		
ID	**Eventos de Risco**	**Causas**	**Consequências**							**Requerida**	**Responsável**	**Situação**
1	-	-	-	-	-	-	-	-	-	-	-	-
2	-	-	-	-	-	-	-	-	-	-	-	-
3	-	-	-	-	-	-	-	-	-	-	-	-

4.6 Comunicação e Consulta

A comunicação e a consulta devem dar-se em processos contínuos e iterativos, capazes de fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas. Têm como objetivo facilitar a troca de informações, levando em consideração os aspectos de confidencialidade, integridade e confiabilidade.

A comunicação e a consulta às partes interessadas acontecem durante todas as fases do processo de gestão de riscos e são direcionadores para a tomada de decisão. É importante que a comunicação observe os agentes e unidades apontadas como consultados ou informados na Matriz RACI do Quadro 2.

Mudanças identificadas durante o monitoramento devem ser encaminhadas à Secretaria de Gestão Estratégica, a quem compete consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento.

A Secretaria de Gestão Estratégica elaborará o Relatório de Monitoramento da Gestão de Riscos do CNMP

com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional. Após análise do Subcomitê, o Relatório deverá ser encaminhado ao Comitê de Governança Corporativa e da Estratégia para apreciação.

5. REFERÊNCIAS

ABNT NBR ISO 31000. **Gestão de riscos**: princípios e diretrizes. Rio de Janeiro/RJ, 2009. Disponível em: <https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf>. Acesso em: 10 maio 2016.

BRASIL. Tribunal Superior do Trabalho. **Política de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/inz6kf>. Acesso em: 10 maio 2016.

_____. _____. **Plano de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/mzAJTK>. Acesso em: 1º jun. 2016.

_____. Ministério do Planejamento Desenvolvimento e Gestão. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**, Brasília/DF, 2017. Disponível em: <http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc/view>. Acesso em: 9 abr. 2018.

_____. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de Gestão de Riscos**, Brasília/DF, 2018. Disponível em: <https://goo.gl/tWgtnA>. Acesso em: 9 abr. 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission.* **Gerenciamento de Riscos Corporativos:** Estrutura Integrada Sumário Executivo. Nova Iorque/EUA, 2007. Disponível em: <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>. Acesso em: 10 maio 2015.

ANEXO I

PLANO DE GESTÃO DE RISCOS DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

(Redação dada pela Portaria CNMP-PRESI nº 214, de 2 de dezembro de 2019)

1. INTRODUÇÃO

No dia 1º de março de 2016, o Comitê de Governança Corporativa e da Estratégia (CGCE), em reunião ordinária, aprovou a criação de Grupo de Trabalho para estudar e propor a Cadeia de Valor e as políticas de gestão de riscos e de segurança institucional do CNMP (GT-Riscos), em atendimento ao Acordão nº 1273/2015–TCU–Plenário e ao disposto no art. 27 da Portaria CNMP-PRESI nº 36, de abril de 2016, revogada pela Portaria CNMP-PRESI nº 25, de fevereiro de 2018. Ao final de dezesseis encontros com profícuos debates sobre o tema, o Grupo concluiu três produtos: a Cadeia de Valor do CNMP (Portaria CNMP-PRESI nº 37, de 18 de abril de 2017); a Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45, de 27 de abril de 2017); e a Política de Segurança Institucional (Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017).

A Cadeia de Valor do CNMP consiste na representação gráfica dos principais macroprocessos que agregam valor à instituição, alinhada à possibilidade de análise das relações entre eles e como cada um deles contribui para o cumprimento das atribuições do órgão. Já as Políticas de Gestão de Riscos e de Segurança Institucional estabelecem objetivos, princípios, diretrizes, recursos, responsabilidades e procedimentos em conformidade com as melhores

práticas adotadas pelo setor público, alinhados com o Planejamento Estratégico e a Cadeia de Valor do CNMP.

Essas iniciativas têm por objetivo minimizar os riscos das principais atividades aqui desenvolvidas e aumentar a segurança da instituição em sua atuação, tendo por consequência maior eficiência na prestação de serviços para a sociedade.

Este documento detalhará a Política de Gestão de Riscos do CNMP, servindo de referência para todas as unidades do CNMP, sem prejuízo da utilização de outras normas complementares específicas relativas à Instituição ou suas unidades. Este plano tem como escopo de aplicação os processos de trabalho do terceiro nível da Cadeia de Valor do CNMP.

Para a elaboração deste documento, foram utilizados planos e manuais de referência, quais sejam, *Enterprise Risk Management – Integrated Framework* (COSO II) e a norma ABNT NBR ISO 31000. Além disso, foi feito *benchmarking* nas seguintes instituições: Tribunal de Contas da União, Ministério do Planejamento, Desenvolvimento e Gestão; Ministério da Transparência e Corregedoria-Geral da União, Tribunal Superior do Trabalho, Tribunal Regional do Trabalho da 18ª Região e Tribunal Regional Eleitoral do Rio Grande do Sul.

2. TERMOS E DEFINIÇÕES

Para fins deste documento, consideram-se os seguintes conceitos:

- Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de comunicação, consulta, estabelecimento do contexto, e, na identificação, análise, avaliação, tratamento, monitoramento e análise crítica dos riscos.
- Objeto de avaliação de riscos: processos de trabalho do terceiro nível da Cadeia de Valor do CNMP.
- Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade.
- Gestor de riscos: pessoa ou entidade com responsabilidade e autoridade para gerenciar um risco.
- Controle interno: conjunto de atividades, planos, métodos, indicadores e procedimentos interligados, estabelecidos com vistas a assegurar que os diversos objetivos das unidades do CNMP sejam alcançados, evidenciando eventuais desvios.
- Contexto externo: ambiente externo no qual a organização busca atingir seus objetivos.
- Contexto interno: ambiente interno no qual a organização busca atingir seus objetivos.
- Eventos de risco: incidente ou uma ocorrência que afeta a realização dos diversos objetivos do CNMP.
- Consequências: resultado de um evento que afeta os diversos objetivos do CNMP.
- Causas: condições que viabilizam a concretização de um evento que afetam os objetivos. São resultantes da junção das fontes de risco com as vulnerabilidades.
- Fonte de risco: elemento que, individualmente ou combinado, tem o potencial intrínseco para dar origem ao risco.
- Vulnerabilidades: Ausência, inadequação ou deficiência em uma fonte de risco, a qual pode vir a contribuir com a concretização de um evento indesejado.
- Nível de risco: magnitude de um risco, expressa em termos da combinação das probabilidades e do impacto.

- Risco: possibilidade que um evento, iminente ou futuro, ocorra e afete negativamente a realização dos objetivos do CNMP.
    - Risco inerente: risco ao qual os processos de trabalho do CNMP estão sujeitos, desconsiderados os controles existentes.
    - Risco residual: risco remanescente após a incidência dos controles aplicados.
    - Risco emergente: risco decorrente da adoção das medidas de controle para um risco inerente ou residual.
- Critérios de risco: padrão de referência para a avaliação dos riscos.
- Apetite a risco: nível de risco que o CNMP se dispõe a aceitar na busca por agregar valor aos serviços prestados.
- Análise de riscos: processo de compreender a natureza do risco e determinar o nível de risco.
- Avaliação de riscos: processo de comparar os resultados da análise de riscos com os critérios de risco para determinar se o risco e/ou sua magnitude é aceitável ou tolerável.
- Tratamento de riscos: abordagem do CNMP após avaliar o risco e, a partir daí, adotar medidas para evitá-lo, transferi-lo/compartilhá-lo, mitigá-lo e, eventualmente, aceitá-lo.
- Medida de controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados.
- Matriz RACI: corresponde à sigla para *Responsible*, *Accountable*, *Consulted* e *Informed* (em português, pode-se traduzir livremente para Responsável, Aprovador, Consultado e Informado). Assim, a matriz RACI é uma ferramenta por meio da qual cada colaborador toma consciência de suas atribuições durante o processo de gestão de riscos. É uma matriz de distribuição de responsabilidades.

3. ESTRUTURA DE GESTÃO DE RISCOS DO CNMP

Segundo a norma ISO 31000, a gestão de riscos em uma organização possui três pilares: os princípios, a estrutura e o processo.

No âmbito do CNMP, nos termos dos art. 3º e 4º da Portaria CNMP-PRESI nº 45, de 27 de abril de 2017, os princípios foram desdobrados em diretrizes e objetivos, respectivamente, conforme quadro abaixo:

Quadro 1 – Diretrizes da Gestão de Riscos do CNMP

Princípios da Gestão de Riscos no CNMP	Diretrizes	• Conformidade dos processos à legislação aplicável • Alinhamento ao Planejamento Estratégico e à Cadeia de Valor • Promoção dos valores institucionais • Disseminação da cultura de gestão de riscos • Adequação do apetite ao risco às estratégias adotadas • Comprometimento das partes envolvidas nos processos organizacionais de tomada de decisões • Dinamismo, iteratividade e capacidade de reagir a mudanças

		• Fomento à melhoria contínua da gestão
	Objetivos	• Identificar potenciais eventos que afetem o alcance da missão institucional • Fornecer informações íntegras para o processo de tomada de decisão • Aprimorar os processos de controle interno

Em relação à estrutura de gestão de riscos, a referida ISO conceitua que é o "*conjunto de componentes que fornecem os fundamentos e os arranjos organizacionais para a concepção, implementação, monitoramento, análise crítica e melhoria contínua da gestão de riscos através de toda a organização".* Ainda dentro da estrutura, a norma mencionada trata dos seguintes componentes: Mandato e Comprometimento, Concepção da Estrutura para Gerenciar Riscos, Implementação da Gestão de Riscos, Monitoramento e Análise Crítica da Estrutura e Melhoria Contínua da Estrutura.

No CNMP, o componente Mandato e Comprometimento é demonstrado pelas ações do Comitê do Governança Corporativa e da Estratégia (CGCE), do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI) e da alta administração em promover a Gestão de Riscos do CNMP.

Na concepção da Estrutura para Gerenciar Riscos, além do CGCE, foi definida a Política de Gestão de Riscos por meio da Portaria CNMP-PRESI nº 45/2017 e foi instituído o SERSI pela Portaria CNMP-PRESI nº 50, de 24 de abril de 2018, normativos que definem o processo de gestão de riscos e as competências e responsabilidades.

Com o entendimento de que os resultados do Monitoramento e da Análise Crítica podem impactar na estrutura e na metodologia de Gestão de Riscos do CNMP, é prevista revisão da Política de Gestão de Riscos e deste Plano em período não superior a dois anos (Melhoria Contínua da Estrutura). Porém, mudanças no contexto do CNMP podem provocar a necessidade de implantação de melhorias de forma antecipada, desde que propostas pelo SERSI e aprovadas pela Secretaria-Geral do CNMP, conforme inciso III do art. 10-E da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018, que altera a Portaria CNMP-PRESI nº 160/2014, instituindo o SERSI no âmbito do CGCE.

3.1. DAS COMPETÊNCIAS

As competências quanto à gestão de riscos do CNMP foram definidas na Política de Gestão de Riscos, na Portaria que institui o SERSI, bem como neste documento. Desse modo, a governança de gestão de riscos configura-se em três níveis:

• nível estratégico com o Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI);

• nível tático com a Secretária de Gestão Estratégica (SGE); e

• nível operacional com o gestor de riscos.

Ressalta-se, ainda, que os níveis de riscos serão tratados em suas respectivas instâncias de governança conforme a Seção 4.4, que define as diretrizes para resposta perante o nível do risco identificado.

3.1.1. Do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional

A principal instância de governança sobre gestão de riscos do CNMP é o SERSI, instituído por meio da Portaria CNMP-PRESI nº 50, de 24 de abril de 2018. Vinculado ao CGCE, o Subcomitê Estratégico é composto por representantes das seguintes unidades: Presidência; Corregedoria Nacional; Secretaria-Geral; Comissões; Secretaria de Gestão Estratégica; Secretaria de Administração; Secretaria Processual; Secretaria de Tecnologia da Informação; Assessoria de Comunicação Social; Auditoria Interna; Coordenadoria Gestão de Pessoas e Coordenadoria de Segurança e Transporte.

As competências do SERSI estão definidas no art. 10-E da Portaria CNMP-PRESI nº 160/2014, quais sejam:

- analisar e deliberar sobre riscos ou ameaças que possam comprometer a prestação de serviços, a imagem junto à sociedade, a autonomia e a efetividade dos resultados no alcance da estratégia;
- monitorar, avaliar e propor a revisão das Políticas de Gestão de Riscos e de Segurança Institucional, periodicamente, submetendo-as à apreciação da Presidência do CNMP;
- elaborar, monitorar, avaliar e propor a revisão do Plano de Gestão de Riscos e do Plano de Segurança Institucional, submetendo-os à deliberação da Secretaria-Geral;
- definir, anualmente, o apetite a riscos do CNMP, conforme previsto na Política de Gestão de Riscos do CNMP; e
- avaliar a eficácia e a efetividade do processo de gerenciamento de riscos e da segurança institucional.

3.1.2. Da Reunião de Acompanhamento Tático (RAT)

A Reunião de Acompanhamento Tático (RAT) é definida na Portaria CNMP-PRESI nº 25/2018 e é realizada entre o secretário-geral, a chefia de gabinete da Presidência e os titulares de secretarias e da Auditoria Interna para riscos afetos à atividade-meio; e entre o secretário-geral, a chefia de gabinete da Presidência e os integrantes da cada Comissão, da Corregedoria Nacional, da Ouvidoria Nacional, da Unidade Nacional de Capacitação do Ministério Público e dos Gabinetes dos conselheiros para riscos afetos à atividade finalística.

3.1.3. Do gestor de riscos

A Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45/2017) define as seguintes competências aos gestores de riscos, relativamente aos objetos de avaliação de riscos sob sua responsabilidade:

- escolher, justificadamente, dentre os objetos (objetivos estratégicos e de contribuição, ações, projetos, iniciativas, ativos e processos de trabalho) sob sua responsabilidade, quais terão os riscos gerenciados, à vista da dimensão dos prejuízos que possam causar;
- assegurar que o risco seja gerenciado de acordo com os critérios do processo de gestão de riscos estabelecidos neste Plano; e
- gerar e reportar informações adequadas sobre a gestão de riscos às instâncias de governança.

Ainda, de acordo com o art. 15 da Portaria CNMP-PRESI nº 45/2017, são considerados **gestores de riscos**, dentre outros, o Presidente, o Corregedor Nacional, o Ouvidor Nacional, os Conselheiros, os presidentes e membros auxiliares das comissões permanentes e temporárias, o Secretário-Geral, os secretários e titulares de unidades administrativas.

3.1.4. Da Secretaria-Geral e da Secretaria de Gestão Estratégica

Compete à Secretaria-Geral presidir o SERSI, realizar estudos e adotar as medidas necessárias para a edição, pela Presidência, de atos normativos dispondo sobre a gestão do conhecimento e a implementação da gestão de riscos e segurança institucional, nos termos do art. 27 da Portaria CNMP-PRESI nº 25/2018.

Para assessorar a SG, segundo o §5º do art. 10-E da Portaria CNMP-PRESI nº 160/2014, a coordenação do processo de gestão riscos do CNMP compete à Secretaria de Gestão Estratégica (SGE). Desse modo, especificam-se as seguintes competências:

- auxiliar o SERSI na definição e nas atualizações da estratégia de implementação da Gestão de Riscos, considerando os contextos externo e interno;
- definir os requisitos funcionais necessários à ferramenta de tecnologia de suporte ao processo de gerenciamento de riscos;
- monitorar a evolução dos níveis de riscos e a efetividade das medidas de controle implementadas;
- dar suporte à identificação, análise e avaliação dos riscos dos processos organizacionais selecionados para a implementação da Gestão de Riscos;
- consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento;
- oferecer capacitação continuada em Gestão de Riscos para os servidores do CNMP;
- promover a disseminação da cultura de gestão de riscos; e
- requisitar aos responsáveis pelo gerenciamento de riscos dos processos organizacionais as informações necessárias para a consolidação dos dados e a elaboração dos relatórios gerenciais.

4. PROCESSO DE GESTÃO DE RISCOS

A gestão de riscos no CNMP explicitada neste documento dar-se-á sobre os processos de trabalho constantes do 3º nível da Cadeia de Valor. Cabe aos gestores de risco, conforme as responsabilidades definidas na Política de Gestão de Riscos, escolher os processos que terão os riscos gerenciados e tratados com prioridade em cada unidade do CNMP, em face da dimensão dos prejuízos que a não gestão dos riscos possa causar. Ainda podem ser levados em

consideração critérios de escolha, tais como: o alinhamento do processo com os objetivos estratégicos do CNMP e o impacto em caso de incidentes ou o custo do processo.

Definido o processo de trabalho, convém ao gestor de riscos elaborar uma matriz RACI, que estabelece as responsabilidades específicas para cada atividade da gestão de riscos em cada unidade. Assim, o responsável (R) é quem efetivamente irá executar a atividade; o aprovador (A) é o responsável pelo aceite formal da atividade ou produto entregue, podendo delegar a função para outros profissionais, mas não a responsabilidade; o consultado (C) é a pessoa que possa fornecer informação sobre a referida atividade; e o informado (I) é a pessoa ou os grupos de pessoas que precisam ser notificados de resultados ou ações tomadas, mas não precisam estar envolvidos no processo de tomada de decisão. O Quadro 2 apresenta um modelo de matriz de responsabilidades (RACI).

Quadro 2 – Matriz RACI para o processo de gerenciamento de riscos

Atividade	SG	SERSI	SGE	Gestor de Riscos	Servidor
Estabelecer o contexto					
Identificar os riscos					
Analisar os riscos					
Avaliar os riscos					
Tratar os riscos					
Elaborar o Plano de Tratamento de Riscos					
Monitoramento e análise crítica					
Comunicar e consultar					
Capacitar envolvidos					

***R** – Responsável; **A** – Aprovador; **C** – Consultado; **I** – Informado*

Uma vez definida a priorização, dar-se-á início ao processo de gestão de riscos, conforme modelo da Norma ABNT NBR 31000:2009, adaptada à realidade do CNMP, com as seguintes atividades:

• estabelecimento do contexto;

• identificação e análise de riscos;

• avaliação de riscos;

• tratamento de riscos;

• monitoramento e análise crítica; e

• comunicação e consulta.

Assim, o processo é composto por 6 (seis) atividades que interagem de forma cíclica. Abaixo, encontra-se a definição de cada atividade e os principais artefatos e atores envolvidos.

4.1. ESTABELECIMENTO DO CONTEXTO

Nesta etapa, devem ser identificados, pelo menos:

- Descrição resumida do processo de trabalho que terá os riscos gerenciados;
- Objetivos a serem alcançados pelo processo de trabalho; e

- Justificativa para a aplicação do processo de gerenciamento de riscos no processo de trabalho.

Também é necessária a definição dos critérios de risco a serem levados em consideração ao gerenciar riscos no CNMP. Essa atividade é de fundamental importância, pois é a partir dela que todas as demais atividades serão desenvolvidas. A fim de deixar o plano mais didático, os critérios de riscos serão definidos ao longo das demais atividades, à medida que forem sendo utilizados.

4.2. IDENTIFICAÇÃO E ANÁLISE DE RISCOS

A identificação dos riscos consiste na busca, no reconhecimento e na descrição de riscos, mediante a identificação das fontes de risco, eventos e suas causas. A finalidade dessa etapa é gerar uma lista abrangente de eventos que possam evitar, prejudicar, impedir ou atrasar o cumprimento dos objetivos do processo de trabalho. A identificação abrangente é fundamental, pois um risco que não é identificado nesta fase não será incluído em análises posteriores.

Nessa fase, o gestor deverá utilizar, como referência, as taxonomias de eventos de riscos e de causas definidas no item 4.2.1. Para a identificação dos riscos, o gestor pode utilizar técnicas como *brainstorming,* entrevista com especialistas, entre outras. Uma vez identificado o risco, o gestor deverá categorizá-lo como estratégico, operacional, de conformidade ou de integridade. Vale ressaltar que um risco pode ser classificado em mais de uma categoria. Destaca-se que essas categorias de riscos estão definidas nos incisos V a VIII do art. 2º da Portaria CNMP-PRESI nº 45/2017.

Identificados e categorizados os riscos, convém analisá-los de forma criteriosa, pois essa análise fornece subsídios para a avaliação de riscos, bem como para as estratégias, métodos e decisões de tratamento dos riscos. A análise envolve a apreciação das causas e das fontes de riscos, suas consequências negativas e a probabilidade de que esses eventos venham a ocorrer.

Nessa etapa, é importante apontar os fatores que afetam as consequências e a probabilidade de ocorrência dos riscos, ou a combinação de ambos, confrontados com os controles existentes, a fim de testar a eficácia e a eficiência desses controles. A combinação das consequências, as quais podem ser expressas em termos de impactos tangíveis e intangíveis, com a probabilidade, serve para determinar o nível do risco inerente.

O Quadro 3 apresenta o Formulário de Identificação e Análise de Riscos:

Quadro 3 – Formulário de Identificação e Análise de Riscos

Processo de trabalho objeto de Avaliação de Riscos:	**Copilado por:** **Data:**
Objetivo do processo de trabalho:	**Analisado por:** **Data:**
Justificativa para o gerenciamento dos riscos:	
Riscos Identificados	

ID	Eventos de Risco	Detalhamento do risco	Causa	Observações sobre a causa	Categoria do risco
1					
2					
3					

4.2.1. Taxonomia de eventos de riscos e de causa

A taxonomia de eventos de riscos está dividida em quinze categorias distintas, compondo o nível 1. Esse nível pode ser subdividido em até dois subníveis de categoria (nível 2 e 3), mutuamente excludentes.

No caso de dúvidas sobre qual das subcategorias adotar na classificação de um evento de risco, considera-se aquele que representa melhor esse evento de risco. Se um evento de risco não tiver condições de ser enquadrado em nenhuma das taxonomias, a equipe do levantamento de riscos pode criar uma nova subcategoria, a qual, posteriormente, será submetida ao SERSI para deliberação.

Quadro 4 – Taxonomia de eventos de riscos

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
1. Fraude Interna	**1.1. Atividade não autorizada**		Perda decorrente de ações não autorizadas, não comunicadas ou realizadas de forma enganosa por membro, servidor, estagiário ou terceirizado, para obter benefício pessoal ou terceiros, violando normas, controles internos e leis, de forma intencional.	Exemplos: vazamento de informações, alteração de dados, conluio, entre outros.
	1.2. Furto		Perda derivada de ato interno intencional com o objetivo de apropriar indevidamente valores financeiros, bens físicos ou informações. Pode incluir apropriação indébita, roubo, furto de informações eletrônicas, entre outros.	Ações de vandalismo devem ser classificadas como "Terrorismo e vandalismo".
2. Fraude Externa	**2.1. Furto e Fraude**		Perda derivada de ato de terceiros com o objetivo de apropriar valores financeiros, bens físicos ou informações do CNMP ou de terceiros, como por exemplo, enviar documentação incorreta ou enganosa.	Exceção: ações de vandalismo e furto de dados via meio eletrônico (classificar em "invasão de sistemas").
	2.2. Invasão de Sistemas		Perda derivada de acesso não autorizado que visa burlar o sistema, explorar suas vulnerabilidades ou furtar dados da instituição ou de seus usuários.	Exemplo: *acking*, ataque de vírus, entre outros.
3. Uso indevido de autoridade	**3.1. Contra o exercício profissional**		Atentar contra os direitos e garantias legais assegurados ao exercício profissional com abuso ou desvio do poder hierárquico ou sem competência legal para atender interesse próprio ou de terceiros. Proceder a qualquer tentativa de obrigar o servidor a executar o que evidentemente não está no âmbito das suas	

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
			atribuições ou a deixar de executar o que está previsto.	
	3.2. Contra a honra e o patrimônio		Atentar contra a honra ou o patrimônio de pessoa natural (no caso, servidor público) ou jurídica com abuso ou desvio de poder ou sem competência legal para atender interesse próprio ou de terceiros.	
4. Nepotismo			Nomear, designar, contratar ou alocar familiar de Conselheiro ou de ocupante de cargo em comissão ou função de confiança para exercício de cargo em comissão, função de confiança ou para a prestação de serviços no CNMP.	
5. Conflito de interesses			Exercício de atividades incompatíveis com as atribuições do cargo; Intermediação indevida de interesses privados; Concessão de favores e privilégios ilegais a pessoa jurídica; Recebimento de presentes/vantagens.	
6. Ameaças à imparcialidade e à autonomia técnica			Ser influenciado a agir de maneira parcial por pressões internas ou externas indevidas, normalmente ocorridas entre pares, por abuso de poder, por tráfico de influência ou constrangimento ilegal.	
7. Conduta profissional inadequada			Deixar de realizar as atribuições conferidas com profissionalismo, honestidade, imparcialidade, responsabilidade, seriedade, eficiência, qualidade e/ou urbanidade.	
8. Uso indevido ou manipulação de dados/ informações			Divulgação ou uso indevido de dados ou informações; alteração indevida de dados/informações; restrição de publicidade ou de acesso a dados ou informações	
9. Desvio de pessoal ou de recursos materiais			Desviar ou utilizar, em obra ou serviço particular, veículos, máquinas, equipamentos ou material de qualquer natureza, de propriedade ou à disposição de entidades públicas, bem como o trabalho de servidores públicos, empregados ou terceiros contratados por essas entidades para fins particulares ou para desempenho de atribuição que seja de sua responsabilidade ou de seu subordinado.	
10. Dano a bens físicos	**10.1. Desastres e outros eventos**	10.1.1 Desastres	Perdas decorrentes de tempestades, erosão, quedas de raios, vendaval, incêndio, explosão, queda de equipamentos, danos de obras, etc.	
		10.1.2 Terrorismo e Vandalismo	Perda decorrente de ações de terrorismo ou vandalismo.	
11. Interrupção de atividade e falha	**11.1. Sistemas**	11.1.1 *Software*/ *Hardware*/ Rede	Inclui indisponibilidade ou falha da rede de processamento, transmissão e de comunicação ou dimensionamento incorreto de hardware.	É válido para sistemas ou equipamentos dos quais a unidade é fornecedor e não usuário. Se

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
de sistema				usuário, tratar como causa TIC
		11.1.2 Telecomunicações	Inclui indisponibilidade ou falha da rede de processamento, transmissão e de comunicação.	
		11.1.3 Serviços de infraestrutura e fornecimentos essenciais	Inclui indisponibilidade de serviços públicos como, por exemplo, fornecimento de eletricidade, água e esgoto, correios, entre outros.	
12. Execução e Gerenciamento de Processos e de Informação	**12.1. Execução e Gerenciamento de Processos**	12.1.1 Erro de informação	Perda ou falha derivada de informações inexatas, incorretas, desatualizadas ou incompletas que são produtos do processo	
		12.1.2. Falha na execução de processos/ práticas de *compliance*	Perda derivada de processamento inadequado ou incorreto de rotinas, procedimentos, sistemas de controle e modelos, de forma não intencional. Também inclui a operacionalização inadequada de sistemas tecnológicos.	Não engloba falha interna no sistema tecnológico decorrente de manutenção ou desenvolvimento. O evento deve ser classificado em como "interrupção de atividades e falha de sistemas".
		12.1.3 Perda de prazo/ atraso atendimento de demandas	Perda ou falha derivada de atividades realizadas fora do horário determinado ou de forma não tempestiva.	
		12.1.4 Erro contábil	Perda derivada de registro contábil não confiável (inexato, incorreto ou incompleto).	
	12.2. Gerenciamento da informação	12.2.1. Erro/ não de divulgação de informação interna	Perda derivada de informações não divulgadas em documentos internos ou de forma não confiável (inexatas, incorretas, incompletas).	Exemplos: comunicados, relatórios, ordens de serviço, Intranet, entre outros.
		12.2.2. Erro/ não de divulgação de informação externa	Perda derivada de informações não divulgadas em documentos externos de forma não confiável (inexatas, incorretas, incompletas).	
	12.3. Fornecedor	12.3.1. Produto/ serviço não conforme	Perda derivada de execução ou entrega defeituosa de produtos e serviços (prazo, qualidade, quantidade, custos).	
		12.3.2. Disputas	Perda relacionada às discordâncias das obrigações contratuais ou legais.	

Nível 1	Nível 2	Nível 3	Descrição do último nível	Observações
		legais		
		12.3.3. Falência	Perdas decorrentes da falência do fornecedor.	
13. Prática Trabalhista e Segurança do Trabalho	**13.1. Recursos Humanos e Cultura**		Perda relacionada com a gestão de pessoal ao longo de todo o ciclo produtivo, desde o recrutamento até o término do vínculo trabalhista, que podem levar à queda de produtividade, dificuldade de retenção, *turnover*, litígio ou processos judiciais.	Pode incluir questões relacionadas com discriminação, assédio, greve, remuneração, reposição de mão de obra, entre outros.
	13.2. Segurança do Trabalho		Perda relacionada com condições e práticas trabalhistas insalubres ou inapropriadas, violência pessoal, perigos relacionados com deslocamento ou viagens a serviço, que afetam a saúde e segurança do servidor, independente da gravidade.	
14. Práticas de Negócio e legal	**14.1. Partes interessadas**	14.1.1. Obrigação legal	Perda derivada de falhas no relacionamento com a população e órgãos públicos decorrente de não cumprimento de leis, regras ou regulamentações.	Inclui mau uso de Informações confidenciais, deixar de cumprir obrigações legais, entre outros.
		14.1.2. Práticas de mercado	Perdas decorrentes do não envio ou do envio de propostas superestimadas ou subestimadas e do fato de o contrato já não ser mais vantajoso para a administração.	
15. Restrições orçamentárias			Perdas derivadas de restrições e contingenciamento orçamentários.	

Para cada risco identificado são também investigadas suas possíveis causas. Podem ocorrer situações em que sejam detectadas mais de uma causa, independente da origem.

Cada causa deve ser classificada com base na taxonomia de causas, que está dividida em causas internas (Quadro 5) e externas (Quadro 6), cada qual com várias subcategorias.

As causas internas são aquelas que surgem dentro da organização e as externas são aquelas que surgem fora da organização.

Quadro 5 – Taxonomia de causas internas

Nível 1	Nível 2	Descrição
1. Recursos Humanos	**1.1. Turnover**	
	1.2. Número de servidores	
	1.3. Gestão do conhecimento institucional	Eventos relacionados a ausência de compilação e valorização dos precedentes (Base de Conhecimento, manuais e enunciados).

Nível 1	Nível 2	Descrição
	1.4. Gestão de competências	Eventos relacionados a deficiências no desenvolvimento de competências e habilidades do servidor e/ou do superior hierárquicos; trabalhos que demandam competências específicas; interpretação equivocada dos normativos, entre outro; ausência de mecanismos de aferição do desempenho dos servidores da organização
	1.5. Greve	
	1.6. Carga de trabalho	Eventos relacionados à incapacidade de gerir o tempo; capacidade operacional insuficiente em relação às demandas, entre outros
	1.7. Clima organizacional	Eventos relacionados à desmotivação, qualidade de vida, saúde do servidor, entre outros.
	1.8. Cultura organizacional	Falta de comprometimento do servidor com os objetivos institucionais e com o serviço prestado; interferência nos trabalhos da equipe por agentes externos (ex: políticos e gestores institucionais).
	1.9. Outros RH	Má-fé do servidor e/ou do superior hierárquico (perseguição, amizade, preferência etc.); o normativo favorece a discricionariedade para a prática do ato; solicitações indevidas indiretas ou diretas por autoridades; pressão familiar; falta de comunicação do servidor quanto à sua suspeição; falta de atenção (não intencional).
2. Tecnologia da Informação		Eventos relacionados à disponibilidade de recursos de TI, como *hardware*, *software*, sistemas obsoletos ou ausentes, demandas internas por recursos de TI e outros.
3. Gerenciamento	**3.1. Planejamento**	Eventos relacionados à formulação das orientações estratégicas e seus desdobramentos (indicadores de desempenho, estabelecimento de metas para as ações, etc.); não aderência às diretrizes e procedimentos da organização, entre outros.
	3.2. Controle	Eventos relacionados ao monitoramento e implementação de controles.
	3.3. Organização	Eventos relacionados à forma de coordenar e adequar os recursos organizacionais.
	3.4. Liderança	Eventos relacionados às competências do líder/gestor em comunicar diretrizes, objetivos, metas; estimular a prática de valores organizacionais; promover a integração das equipes e com outros componentes do CNMP; tomar decisões; articular interesses; priorizar ações; inovar; delegar; resolver conflitos, entre outros.
	3.5. Outros Gerenciamento	Deficiências nos fluxos dos processos de trabalho e de informações entre as unidades da organização; fragilidade no processo de comunicação de informações produzidas ou custodiadas pelo CNMP
4. Recursos Financeiros		Eventos relacionados com indisponibilidade de recursos financeiros.

Nível 1	Nível 2	Descrição
5. Recursos Materiais		Eventos relacionados com qualidade inadequada, carência de recursos materiais ou obsolescência.
6. Segurança Institucional		Eventos relacionados à segurança orgânica (segurança de pessoas, de materiais, das áreas e instalações e de informação) e segurança ativa, tais como sabotagem, propaganda adversa e espionagem.
7. Regulação		Eventos relacionados com mudanças no ambiente legal e regulatório.

Quadro 6 – Taxonomia de Causas Externas

Nível 1	Descrição
1. Econômica	Eventos relacionados com mudança do ambiente econômico.
2. Política	Eventos relacionados com fatores do ambiente político que podem comprometer os resultados do macroprocesso, projeto ou iniciativa.
3. Regulação	Eventos relacionados com mudanças no ambiente legal e regulatório.
4. Energia elétrica	Eventos relacionados à disponibilidade de fornecimento de energia elétrica.
5. Telecomunicações	Eventos relacionados à disponibilidade de fornecimento de telecomunicações.
6. Terceiros	Eventos decorrentes da relação com terceiros.
7. Fornecedores	Eventos decorrentes da relação com fornecedores (relação contratual).

4.3. AVALIAÇÃO DE RISCOS

A finalidade da avaliação de riscos é auxiliar na tomada de decisões, com base nos resultados das etapas anteriores, sobre quais riscos necessitam de tratamento e a prioridade para a implementação das ações de tratamento do risco.

A avaliação de riscos envolve comparar o nível de risco encontrado durante o processo de análise com os critérios do processo de gestão do CNMP, quais sejam: probabilidade, impacto, apetite a riscos, matriz de classificação de riscos, diretrizes para priorização e tratamento, e matriz da eficácia dos controles.

A probabilidade diz respeito às chances de um evento ocorrer. Dessa forma, o Quadro 7 define os graus de probabilidade e os respectivos níveis.

Quadro 7 – Escala de probabilidade

Descritor	Descrição	Nível
Muito baixa	Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.	1
Baixa	Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.	2
Média	Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.	3

Alta	Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.	4
Muito alta	Praticamente certa. De forma inequívoca, o evento ocorrerá, pois as circunstâncias indicam claramente essa possibilidade.	5

Fonte: Adaptado de Plano de Gestão de Riscos (TST, 2015)

O impacto, por sua vez, está relacionado às consequências do evento nos objetos, caso ele ocorra. Visando a diminuir a subjetividade do método, optou-se por definir o nível desse impacto considerando as dimensões financeira, reputacional e de negócios no objetivo do processo de trabalho analisado.

Para cada cruzamento de risco é feita a avaliação dos impactos dos eventos identificados nas três dimensões:

1. **Impacto na dimensão financeira:** O impacto na dimensão financeira avalia a perda financeira gerada pelo evento de risco como, por exemplo, pagamento de multas, litígios, compensações, custas legais, negociações mal concluídas, ressarcimento de danos de bens, etc.

2. **Impacto na dimensão reputacional:** Do ponto de vista da dimensão reputacional, avalia-se como um evento de risco pode prejudicar a reputação e credibilidade do CNMP. O efeito reputacional adverso deve estar vinculado à imagem externa do CNMP, ou seja, sua imagem perante o Ministério Público, fornecedores, órgão de governo, parceiros e a sociedade em geral.

3. **Impacto na dimensão de negócios:** Na dimensão de negócios, busca-se avaliar se a ocorrência de um evento compromete o negócio a ponto de afetar a entrega de um produto ou serviço, inclusive aqueles intimamente relacionados ao planejamento estratégico ou até o cumprimento da missão. Para avaliar o impacto na dimensão negócio, devem ser consideradas as definições de missão, visão e planejamento estratégico.

Desse modo, primeiramente o gestor deve analisar o impacto nessas dimensões, conforme quadro abaixo:

Quadro 8 – Escala de impacto

Financeiro	Reputacional	Negócios	Nível
Impacto foi insignificante.	Impacto insignificante.	Impacto insignificante.	1
Perda ou estimativa até R$20.000 (x <= R$20.000).	Eventos que se limitam às partes envolvidas, tenham caráter pontual e/ou não tenham sido divulgados em qualquer mídia.	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance das metas do processo.	2
Perda ou estimativa entre R$20.000 e R$176.000 (R$ 20.000 < x <= R$ 176.000).	Eventos que envolvam membros ou gestores do CNMP, tenham impactos de curto prazo e/ou tenham alcançado mídias institucionais do Ministério Público.	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance dos objetivos do CNMP.	3
Perda ou estimativa de perda entre R$176.000 a R$1.430.000	Eventos que envolvam a Presidência, os Conselheiros, a Corregedoria e/ou a Secretaria-	O evento de risco impacta na entrega do produto ou serviço de tal	4

(R$176.000 < x <= R$ 1.430.000).	Geral, tenham impacto de médio prazo e/ou alcançado a mídia nacional.	forma que prejudica o alcance da visão do CNMP.	
Perda ou estimativa de perda maior que R$1.430.000 (x > R$ 1.430.000).	Eventos que envolvam a Presidência, os Conselheiros, a Corregedoria e/ou a Secretaria-Geral, tenham impacto de longo prazo e/ou tenham alcançado a mídia internacional	O evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance da missão do CNMP.	5

Fonte: Adaptado do BCB

Em relação ao Quadro 8, pode ocorrer de os níveis serem diferentes para cada dimensão. Nesse caso, o gestor de riscos deve considerar o nível mais alto. Por exemplo, caso na dimensão Financeira o gestor considere que o impacto é insignificante (nível 1) e na dimensão Negócios considere que o evento de risco impacta na entrega do produto ou serviço de tal forma que prejudica o alcance das metas do processo (nível 2), o nível de impacto a ser considerado será o 2.

Tendo em mãos os níveis de probabilidade e impacto, o gestor de riscos deve fazer a multiplicação desses níveis, que define o nível do risco inerente, ou seja, o nível do risco sem considerar quaisquer controles que reduzem ou podem reduzir a probabilidade da sua ocorrência ou do seu impacto.

O risco pode ser classificado dentro das seguintes faixas:

Quadro 9 – Classificação do risco

Classificação	Faixa
Risco Baixo	0 – 4,99
Risco Médio	5,00 – 9,99
Risco Alto	10,00 – 14,99
Risco Extremo	15,00 – 25,00

Fonte: Adaptado de Gestão de Riscos – Avaliação da Maturidade (TCU, 2018)

Quadro 10 – Matriz de riscos

Nível de Risco **Extremo** **Alto** **Médio** Baixo		**PROBABILIDADE**				
		Muito baixa 1	**Baixa 2**	**Média 3**	**Alta 4**	**Muito alta 5**
IMPACTO	**Muito alto 5**	5	10	15	20	25
	Alto 4	4	8	12	16	20

	Médio 3	3	6	9	12	15
	Baixo 2	2	4	6	8	10
	Muito baixo 1	1	2	3	4	5

Para finalizar os critérios de riscos, o CNMP definiu a Tabela da Eficácia dos Controles Existentes (Quadro 11), a qual estabelece critérios objetivos para análise dos controles implementados e para cálculo do risco residual. Esse quadro deve ser aplicado logo após a definição dos níveis de riscos, caso já existam controles implementados, e após a adoção das medidas de tratamento dos riscos.

Quadro 11 – Eficácia dos controles existentes

Eficácia do Controle	**Situação do controle**	**Multiplicador do Risco Inerente**
Inexistente	Ausência completa de controle.	1,0
Fraco	Controle parcialmente implantado e com deficiências. Geralmente depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado de maneira manual.	0,8
Mediano	Controle parcialmente implantado. Entretanto, pode falhar por não contemplar todos os aspectos relevantes do risco ou porque seu desenho ou as ferramentas que o suportam não são adequados.	0,6
Satisfatório	Controle implantado e executado de maneira periódica e quase sempre uniforme. Avaliação dos controles é feita com alguma periodicidade.	0,4
Forte	Controle implantado e executado de maneira uniforme pela equipe e na frequência desejada. Periodicamente os controles são testados e aperfeiçoados.	0,2

Fonte: Plano de Gestão de Riscos (TST, 2015)

Ressalta-se, também, que o apetite a risco do CNMP levará em consideração o risco no nível baixo, ou seja, para riscos nesse nível, não há a necessidade de ações e medidas de tratamento. Assim, basta apenas o seu monitoramento constante para assegurar que eles ainda se encontram nesses patamares.

O Quadro 12 representa o Formulário de Avaliação de Riscos:

Quadro 12 – Formulário de Avaliação de Riscos

Processo de trabalho objeto de Avaliação de Riscos:								**Compilado por:** **Data:**			
Objetivo do processo de trabalho:								**Analisado por:** **Data:**			
Riscos Identificados					**Probabilidade**	**Impacto**	**Risco Inerente**	**Controles Existentes**			**Risco Residual**
ID	**Eventos de Risco**	**Detalhamento do risco**	**Causa**	**Observações sobre a causa**				**Descrição**	**Eficácia**		
1											
2											

4.4. TRATAMENTO DE RISCOS

Nesta etapa, devem ser considerados os valores dos níveis de riscos residuais calculados na etapa anterior para definir as diretrizes para respostas consoante quadro a seguir:

Quadro 13 – Diretrizes para resposta perante o nível do risco

Nível de Risco	Descrição	Diretriz para Resposta
Extremo	Nível de risco muito além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação pelo Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI).	Qualquer risco encontrado nessa área deve ter uma resposta imediata. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 15 dias. O plano de ação deverá ser apreciado pelo Subcomitê, aprovado pelo Secretário-Geral e implementado em até 3 meses. O monitoramento será feito no Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos, apreciação do Subcomitê e aprovação do Secretário-Geral.
Alto	Nível de risco além do apetite a risco. Qualquer risco nesse nível deve ser objeto de avaliação da Reunião de Acompanhamento Tático (RAT).	Qualquer risco encontrado nessa área deve ter uma resposta em até 15 dias. O gestor de risco deverá apresentar plano de ação de tratamento do risco no prazo máximo de 30 dias. O plano de ação deverá ser apreciado na Reunião de Acompanhamento Tático (RAT), aprovado pelo Secretário-Geral e implementado em até 6 meses. O monitoramento será feito na Reunião de Acompanhamento Tático (RAT). Admite-se postergar o tratamento somente mediante parecer do gestor de riscos e aprovação do Secretário-Geral.
Médio	Nível de risco além do apetite a risco. Geralmente nenhuma medida especial é necessária, porém requer atividades de monitoramento específicas e atenção da unidade na manutenção de respostas e controles para manter o risco nesse nível, ou reduzi-lo sem custos adicionais.	O gestor de riscos da unidade deve adotar medidas de tratamento no decorrer de um ano. O monitoramento será feito nas RAOs.
Baixo	Nível de risco dentro do apetite a risco, onde há possíveis oportunidades de maior retorno que podem ser exploradas.	Explorar as oportunidades se determinado pelo gestor de riscos.

As ações de tratamento de riscos são: evitar o risco, não iniciando ou descontinuando a atividade que dá origem ao risco; mitigar o risco, implantando controles que diminuam a probabilidade de ocorrência do risco ou suas consequências; aceitar o risco, assumindo o risco, por escolha consciente e justificada, pois ou o nível do risco é considerado baixo ou a capacidade da organização para tratar o risco é limitada ou o custo é desproporcional ao benefício; e transferir o risco, compartilhando ou transferindo o risco com outra parte interessada.

O tratamento de riscos envolve a seleção de uma ou mais opções para modificar os riscos. A implementação do tratamento pode gerar novos controles ou modificar os controles existentes. A fase inicial do tratamento de riscos é a elaboração do Plano de Tratamento de Riscos, que deve levar em consideração a eficácia das ações já existentes, as restrições organizacionais, técnicas e estruturais, os requisitos legais, a análise custo-benefício e as ações a serem realizadas. Além disso, no Plano de Tratamento de Riscos devem constar os responsáveis, as prioridades e os prazos de execução.

Quadro 14 – Plano de Tratamento de Riscos

Processo de trabalho objeto de Avaliação de Riscos:								**Compilado por:** **Data:**		
Objetivo do processo de trabalho:								**Analisado por:** **Data:**		
Riscos Prioritários				**Categoria do Risco**	**Tipo de Tratamento**	**Ações e Medidas de Tratamento**	**Relação Custo-Benefício**	**Responsável**	**Período de Execução**	**Monitoramento do Risco e seu Tratamento**
ID	**Eventos de Risco**	**Causas**	**Observações sobre a causa**							
1										
2										
3										

4.5. MONITORAMENTO E ANÁLISE CRÍTICA

A fase de monitoramento e análise crítica acontecerá nas reuniões do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional, nas Reuniões de Acompanhamento Tático, nas Reuniões Acompanhamento Operacional e por meio do gestor de riscos, periodicamente ou quando acontecer em resposta a um fato específico.

Entre as finalidades do monitoramento e análise crítica estão a garantia de que os controles sejam eficazes e eficientes, a obtenção de informações adicionais para melhorar a avaliação dos riscos e identificar os riscos residuais que poderão surgir após o processo de análise crítica, reiniciando o ciclo do processo.

O Quadro 15 representa o Formulário de Monitoramento e Análise.

Quadro 15 – Formulário de Monitoramento e Análise

Processo de trabalho objeto de Avaliação de Riscos:						**Compilado por:** **Data:**						
Objetivo do processo de trabalho:						**Analisado por:** **Data:**						
Risco				**Categoria do Risco**	**Controles existentes**	**Data**	**Ocorrência do Risco**	**Novos controles**	**Risco Residual**	**Melhoria**		
ID	**Eventos de Risco**	**Causas**	**Observações sobre a causa**							**Requerida**	**Responsável**	**Situação**
1												
2												
3												

4.6. COMUNICAÇÃO E CONSULTA

A comunicação e a consulta devem dar-se em processos contínuos e iterativos, capazes de fornecer, compartilhar ou obter informações e se envolver no diálogo com as partes interessadas. Têm como objetivo facilitar a troca de informações, levando em consideração os aspectos de confidencialidade, integridade e confiabilidade.

A comunicação e a consulta às partes interessadas acontecem durante todas as fases do processo de gestão de riscos e são direcionadores para a tomada de decisão. É importante que a comunicação observe os agentes e unidades apontadas como consultados ou informados na Matriz RACI do Quadro 2.

Mudanças identificadas durante o monitoramento devem ser encaminhadas à Secretaria de Gestão Estratégica, a quem compete consolidar os resultados das diversas unidades em relatórios gerenciais e encaminhá-los às instâncias de governança e monitoramento.

A Secretaria de Gestão Estratégica elaborará o Relatório de Monitoramento da Gestão de Riscos do CNMP com a consolidação desses resultados, que deve ser encaminhado, no mínimo, uma vez por ano ao Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional. Após análise do Subcomitê, o Relatório deverá ser encaminhado ao Comitê de Governança Corporativa e da Estratégia para apreciação.

5. REFERÊNCIAS

ABNT NBR ISO 31000. **Gestão de riscos**: princípios e diretrizes. Rio de Janeiro/RJ, 2009. Disponível em: <https://gestravp.files.wordpress.com/2013/06/iso31000-gestc3a3o-de-riscos.pdf>. Acesso em: 10 maio 2016.

BRASIL. Tribunal Superior do Trabalho. **Política de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/inz6kf>. Acesso em: 10 maio 2016.

_____. _____. **Plano de Gestão de Riscos**, Brasília/DF, 2015. Disponível em: <https://goo.gl/mzAJTK>. Acesso em: 1º jun. 2016.

_____. Ministério do Planejamento Desenvolvimento e Gestão. **Manual de Gestão de Integridade, Riscos e Controles Internos da Gestão**, Brasília/DF, 2017. Disponível em: <http://www.planejamento.gov.br/assuntos/gestao/controle-interno/manual-de-girc/view>. Acesso em: 9 abr. 2018.

_____. Ministério da Transparência e Controladoria-Geral da União. **Metodologia de Gestão de Riscos**, Brasília/DF, 2018. Disponível em: <https://goo.gl/tWgtnA>. Acesso em: 9 abr. 2018.

COSO. *Committee of Sponsoring Organizations of the Treadway Commission.* **Gerenciamento de Riscos Corporativos:** Estrutura Integrada Sumário Executivo. Nova Iorque/EUA, 2007. Disponível em: <https://www.coso.org/Documents/COSO-ERM-Executive-Summary-Portuguese.pdf>. Acesso em: 10 maio 2015.

ANEXO II

PORTARIA CNMP-PRESI Nº 167, DE 30 DE NOVEMBRO DE 2018.

PLANO DE SEGURANÇA INSTITUCIONAL DO CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

1. INTRODUÇÃO

O presente documento trata do Plano de Segurança Institucional (PSI) do Conselho Nacional do Ministério Público elaborado pelo Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI).

O Plano de Segurança Institucional consiste no detalhamento das diretrizes, dos objetivos e das medidas de segurança institucional constantes da Política de Segurança Institucional do CNMP, além de estabelecer competências e transmitir orientações setoriais e individuais acerca de segurança institucional para os integrantes do Conselho Nacional do Ministério Público.

Sua implementação está fundamentada na Resolução CNMP nº 156, de 13 de dezembro de 2016; na Cadeia de Valor do CNMP (Portaria CNMP-PRESI nº 37, de 18 de abril de 2017); na Política de Gestão de Riscos do CNMP (Portaria CNMP-PRESI nº 45, de 27 de abril de 2017); e, principalmente, na Política de Segurança Institucional (Portaria CNMP-PRESI nº 153, de 7 de dezembro de 2017).

A Segurança Institucional tem caráter essencial e permanente. Deve-se buscar a promoção de atividades para capacitação e aperfeiçoamento dos servidores públicos. Para tanto, deve ser promovida a realização de cursos, seminários, palestras e quaisquer outras atividades que contribuam para o desenvolvimento da segurança institucional.

2. TERMOS E DEFINIÇÕES

Para fins deste documento, consideram-se os seguintes conceitos:

• Segurança Institucional: é o conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações de qualquer natureza que constituam ameaça à salvaguarda da Instituição e de seus integrantes, inclusive à imagem e reputação.

• SERSI: Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional.

• Plano de Emergência: os planos de emergência estabelecem as diretrizes e ações a serem realizadas no caso de ocorrerem emergências que possam repercutir na segurança da instituição e de seus integrantes. Eles apresentam procedimentos de resposta às situações emergenciais, definem atribuições e estabelecem as condições de execução das ações previstas.

• Planejamento de Contingência: compreende um conjunto de medidas voltadas a minimizar ou neutralizar os impactos decorrentes da interrupção de atividades críticas e serviços essenciais do CNMP ocasionada por falhas, desastres, indisponibilidade significativa ou ação intencional de ator hostil em processos sensíveis, permitindo a continuidade das atividades e serviços em níveis aceitáveis. Esse planejamento contempla ações de prevenção e recuperação, além de medidas de avaliação do dano, que constituem os planos de contingência e os planos de controle de danos.

• Contrassabotagem: compreende um conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar ações intencionais contra material, áreas ou instalações da Instituição que possam causar interrupção de suas atividades e/ou impacto físico direto e psicológico indireto sobre seus integrantes, Portaria CNMP/PRESI nº 153/2017.

• Contraespionagem: compreende um conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de ações adversas e dissimuladas de busca de informações sensíveis ou sigilosas, Portaria CNMP/PRESI nº 153/2017.

• Contrapropaganda: compreende um conjunto de medidas voltadas a prevenir, detectar, obstruir e neutralizar o risco de abusos, desinformações e publicidade enganosa de qualquer natureza contra a Instituição, Portaria CNMP/PRESI nº 153/2017.

• Engenharia Social: é definida como a utilização de práticas manipulatórias com fins de contornar dispositivos de segurança ou de obter informações sigilosas ou sensíveis, explorando a confiança das pessoas para enganá-las.

• Recurso de Tecnologia da Informação: compõem os equipamentos e infraestrutura de rede de dados em uso institucional pelo CNMP, tais como: a rede de dados local, seus equipamentos e serviços; a rede de dados sem fio, seus equipamentos e serviços; os microcomputadores de mesa, portáteis e seus dispositivos periféricos; dispositivos móveis institucionais (tablets e smartphones); os softwares adquiridos e os sistemas desenvolvidos no órgão; as informações armazenadas, inclusive as mensagens nas caixas de correio eletrônico institucionais, e em tráfego na rede local; os canais de comunicação com a internet; os suprimentos e bens de consumo relacionados à tecnologia da informação.

• Usuário de Recurso de Tecnologia da Informação: todo membro, servidor, terceirizado, estagiário ou pessoa que, em razão de trabalho de interesse do CNMP, precise de acessos aos recursos de tecnologia da informação.

• Classificação de informação: atribuição a documentos, ou às informações neles contidas, de graus de sigilo, conforme legislação específica. Também chamada classificação de segurança.

• Gestão de documentos: conjunto de procedimentos e operações técnicas referentes à produção tramitação, uso, avaliação e arquivamento de documentos em fase corrente e intermediária, visando à sua eliminação ou recolhimento.

3. DAS ATRIBUIÇÕES

A segurança institucional possui caráter sistêmico, o que enseja a participação de todas as unidades que compõem este Conselho, devendo atuar de forma integrada, visando a atingir os objetivos de segurança.

As decisões acerca de Segurança Institucional caberão ao gestor de segurança institucional, que será o titular da Secretaria-Geral, apoiado pelo SERSI e, quando necessário, pela Secretaria de Administração, assessorada pela Coordenadoria de Segurança e Transporte.

A implementação das normas de segurança institucional será de responsabilidade de todos os conselheiros, membros auxiliares, servidores, estagiários e terceirizados.

3.1 Das Atribuições da Secretaria de Administração, assessorada pela Coordenadoria de Segurança e Transporte:

I - Assessorar a Secretaria-Geral na aplicação das medidas de segurança;

II - Solicitar auxílio aos órgãos de segurança pública, quando for o caso, nos incidentes de segurança;

III - Promover a proteção, quando solicitado pela Secretaria-Geral, de membros, servidores e seus familiares em situação de risco decorrente do exercício da função, conforme Resolução nº 156, de 13 de dezembro de 2016;

IV - Promover a conscientização dos integrantes da Instituição quanto à importância da segurança institucional, incluindo a divulgação do PSI;

V - Coordenar, orientar, supervisionar e fiscalizar as atividades de segurança institucional do CNMP, bem como a implementação do PSI;

VI - Auxiliar a Secretaria-Geral na busca de informações com vistas a subsidiar as atividades de segurança institucional;

VII - Consolidar novas proposições na área de segurança e submetê-las ao SERSI, a partir de demandas existentes;

VII - Levar imediatamente ao conhecimento do Gestor de Segurança Institucional todo e qualquer incidente de segurança;

VIII - Promover a interação com órgãos de segurança pública, visando ao compartilhamento de informações que possam auxiliar as atividades da área de segurança do CNMP, bem como a cooperação tecnológica;

IX - Instaurar procedimento de Análise de Risco sempre que um colaborador do CNMP se sentir ameaçado em virtude de sua função, a fim de dimensionar a probabilidade de ocorrência de uma ameaça e a intensidade de seu impacto;

X - Prover a segurança física de membros e servidores, quando solicitada, na realização de avaliações, vistorias, perícias, inspeções, correições e auditorias, bem como em qualquer outra situação que apresente risco à integridade física dos colaboradores;

XI - Elaborar Procedimento Operacional Padrão (POP) que ampare as ações referentes ao planejamento para emergências, bem como o plano de contingência e controle de danos; e

XII - Delegar ao coordenador da área de segurança a prática dos atos necessários à implementação deste PSI.

3.2 Das Atribuições do Subcomitê Estratégico de Gestão de Riscos e Segurança Institucional (SERSI)

I - Analisar e deliberar sobre riscos ou ameaças que possam comprometer a prestação de serviços, a imagem junto à sociedade, a autonomia e a efetividade dos resultados no alcance da estratégia;

II - Elaborar, monitorar, avaliar e propor a revisão da Política de Segurança Institucional e do Plano de Segurança Institucional, submetendo-os à deliberação da Secretaria-Geral; e

III - Avaliar a eficácia e a efetividade do processo da segurança institucional.

4. DOS PROCESSOS DE SEGURANÇA INSTITUCIONAL

As dimensões que integram a segurança institucional devem funcionar de forma integrada e coordenada, tendo em vista que envolvem o órgão como um todo. Essas dimensões se dividem em: segurança orgânica e ativa.

4.1 Segurança Orgânica

A segurança orgânica é o conjunto de medidas de segurança de pessoas, segurança de material, segurança de áreas e instalações e segurança da informação, esta última se fragmenta em segurança da informação de pessoas, segurança da informação na documentação, segurança da informação nas áreas e instalações e segurança da informação nos recursos de tecnologia da informação, conforme abordado na Portaria CNMP-PRESI N°153, de 7 de dezembro de 2017.

a) Segurança de Pessoas: A segurança de pessoas é um conjunto de medidas destinadas a proteger a integridade física dos integrantes do CNMP, assim como de seus respectivos familiares, quando comprometida em face dos riscos, concretos ou potenciais, decorrentes do desempenho das funções institucionais. A segurança de pessoas, entre outras ações, abrange as operações de segurança, atividades planejadas e coordenadas, com emprego de pessoal, material, armamento e equipamento especializado e subsidiadas por conhecimento de inteligência a respeito da situação.

Pela natureza e circunstâncias do trabalho, é fundamental que os integrantes do CNMP desenvolvam uma cultura de sensibilização e conscientização quanto às prováveis ameaças, estabelecendo procedimentos de proteção e preservação de sua integridade física e dos demais servidores e membros.

Todos devem respeito às normas de segurança de pessoas do CNMP e observância às seguintes recomendações:

I - Não fornecer dados pessoais de integrantes do CNMP sem autorização;

II - Não informar aos solicitantes horários de chegada, saída ou presença de integrantes do CNMP sem antes solicitar autorização para tal;

III - Não permitir visita à integrantes do CNMP sem prévia autorização do interessado;

IV - Não revelar dados pessoais que possam comprometer a segurança individual em redes de dados (internet e intranet);

V - Comunicar aos responsáveis pela segurança qualquer ameaça à integridade física dos colaboradores, para adoção de medidas cabíveis; e

VI - Interromper suas tarefas, nos casos de acionamento do alarme de incêndio, e dirigir-se às saídas de emergência, atendendo às orientações das equipes de brigada e combate a incêndio e de segurança da instalação física.

b) Segurança de Materiais: A segurança de materiais é um conjunto de medidas de segurança voltadas a proteger o patrimônio físico do CNMP, incluindo equipamentos, componentes, acessórios, mobiliários, veículos, matérias-primas e demais itens empregados nas atividades da Instituição. Tem por objetivo salvaguardar a produção, o recebimento, a distribuição, o manuseio, o armazenamento, o

transporte, o descarte, o desfazimento e o acondicionamento dos materiais e equipamentos de posse ou sob a responsabilidade do CNMP.

I - No controle dos bens, da sua movimentação e do seu desfazimento, deve ser observada a Portaria CNMP-SG Nº 271, de 1º de dezembro de 2017, e as orientações do PSI;

II - É proibida a saída de bens do CNMP sem a devida autorização;

III - A movimentação de bens patrimoniais, oriundos do depósito, será precedida de autorização e acompanhamento da Área de Patrimônio;

IV - A saída e o retorno de material do CNMP devem atender normas administrativas e constar em registro, mantido pela área de segurança, em conjunto com os demais setores;

V - Todos os setores devem observar o devido cuidado com a guarda e o correto manuseio dos equipamentos sob a sua responsabilidade; e

VI - A utilização de bens particulares eletroeletrônicos e/ou inflamáveis que possam causar danos às pessoas e ao patrimônio do CNMP deve ocorrer de acordo com os critérios estabelecidos pelas áreas técnicas.

c) Segurança de Áreas e Instalações: Nos termos do art. 6º da Resolução CNMP nº 156, de 13 de dezembro de 2016, a segurança de áreas e instalações constitui-se em um grupo de medidas orientadas para proteger o espaço físico sob responsabilidade do CNMP ou onde se realizem atividades de interesse da Instituição, bem como seus perímetros, com a finalidade de salvaguardá-las.

O grupo de medidas da segurança de áreas e instalações interage com os demais grupos de medidas de segurança e é composto por procedimentos, estruturas e princípios que objetivam preservar a incolumidade física de ativos e passivos da instituição, tais como:

• Gestão de segurança dos perímetros internos e adjacentes à edificação;

• Controle de acesso de pessoas e veículos às dependências da instituição; e

• Controle de entrada e saída de bens e materiais nas dependências do CNMP.

O acesso de pessoas armadas nas áreas e instalações do CNMP deve atender aos critérios previstos na Portaria CNMP-PRESI nº 272, de 15 de agosto de 2013.

As aquisições, ocupação, uso e aluguéis de imóveis, e os projetos de construção, adaptação e reforma de áreas e instalações devem ser planejados e executados com a observância dos aspectos e diretrizes de segurança institucional, e com a integração dos demais setores da instituição, de modo a reduzir as vulnerabilidades e riscos, aprimorando, assim, os meios de proteção.

As áreas e instalações que abriguem informações sensíveis ou sigilosas e as consideradas vitais para o pleno funcionamento da instituição serão objeto de especial proteção.

Compõem os sistemas integrados de proteção:

I - Sistema de videomonitoramento, que possibilita a vigilância remota do perímetro interno e adjacente ao CNMP;

II - Sistema de alarme, composto por equipamentos de sinalização sonora ou luminosa que visam a alertar sobre situações anormais de segurança;

III - Sistema de detecção de movimento, composto por equipamentos que visam a detectar remotamente a movimentação de pessoas, animais ou objetos nas áreas de segurança das instalações físicas;

IV - Controle de acesso, efetivado por meio de mecanismos físicos ou eletrônicos de triagem do

acesso às instalações físicas; e

V - Saídas de emergência, a serem utilizadas em casos de evacuação.

d) Segurança da Informação: A segurança da informação compreende a proteção da informação contra ameaças à confidencialidade, integridade, disponibilidade e autenticidade, para minimizar riscos, garantir a eficácia dos processos de negócio e preservar a imagem do CNMP.

A segurança da informação no CNMP alinha-se às estratégias organizacionais e aos princípios da segurança institucional e tem como princípios:

I - Garantia da integridade e da autenticidade das informações produzidas;

II - Preservação da integridade e da autenticidade das informações recebidas;

III - Transparência das informações públicas;

IV - Proteção adequada às informações com necessidade de restrição de acesso;

V - Planejamento das ações de segurança da informação por meio de uma abordagem baseada em riscos; e

VI - Garantia da disponibilidade das informações custodiadas.

d.1) Segurança da Informação de pessoas: A segurança da informação de pessoas refere-se ao grupo de medidas voltadas a assegurar a proteção de informações sensíveis ou sigilosas dos integrantes do CNMP. Esse grupo de medidas, que abarca as ações relacionadas à segurança no processo seletivo, no desempenho da função e no desligamento da função ou da Instituição, além de ser de responsabilidade de todos, tem como objetivo:

I - Detectar, prevenir e gerenciar as infiltrações, recrutamentos e outras ações adversas de obtenção indevida de informações;

II - Identificar, de maneira precisa, atualizada e detalhada, as pessoas em atuação no CNMP;

III - Verificar e monitorar as ações de prestadores de serviços à Instituição; e

IV - Promover a cultura comportamental de combate a ataques de engenharia social.

d.2) Segurança da Informação na Documentação: A segurança da informação na documentação compreende o conjunto de medidas voltadas a proteger informações sensíveis ou sigilosas contidas na documentação que é arquivada ou tramita na Instituição. Tais medidas deverão ser adotadas em cada fase de produção, classificação, tramitação, difusão, arquivamento e destruição da documentação.

Os documentos deverão ser classificados de acordo com o grau de sigilo exigido por seu conteúdo, de forma a assegurar que recebam nível adequado de proteção. A Instituição deverá adotar os procedimentos que garantam uma gestão documental adequada para documentos ostensivos e sigilosos, inclusive com o estabelecimento dos respectivos protocolos de segurança.

d.2.1) Segurança na Gestão dos Documentos:

I - O programa de gestão de documentos é único e serve para documentos digitais e não digitais, e consiste em um conjunto de procedimentos e operações técnicas referentes à produção, tramitação, uso, avaliação e arquivamento dos documentos em fase corrente e intermediária, visando à sua eliminação ou recolhimento para guarda permanente;

II - A gestão dos documentos digitais, assim como a dos não digitais, terá como base o Plano/Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos, aprovados pela

autoridade competente, e só serão eliminados mediante procedimento formal instaurado, após cumpridos os prazos de guarda previstos;

III - O CNMP deve definir uma política de gestão de arquivo documental que tenha por objetivo produzir, manter e preservar documentos confiáveis, autênticos, acessíveis e compreensíveis, de maneira a apoiar suas funções e atividades;

IV - Todas as áreas de armazenamento de documentos e arquivos físicos devem estar seguras. Elas devem ser mantidas trancadas, e a entrada deve ser feita por chave ou dispositivo interno de segurança, de modo que o acesso seja apenas para servidores autorizados e estritamente controlado pelo responsável;

V - O acesso à informação sobre a localização de documentos físicos dentro do arquivo também será restrito aos servidores autorizados;

VI - Os sistemas de gestão de documentos eletrônicos devem possuir medidas de segurança como: cópias de segurança, controle de acesso, classes de sigilo, trilhas de auditoria, criptografia e assinatura digital para preservar a autenticidade das informações que serão controladas e protegidas; e

VII - Os sistemas informatizados utilizados para a produção dos documentos digitais devem possuir funcionalidades e estar adequados para apoiar a política de preservação digital do CNMP, que preveja estratégias como: conversão, normalização, atualização de suporte, escolha dos formatos de arquivo produzidos, monitoramento de formatos e de mídias, definição de metadados, dentre outros.

• Classificação de Segurança

A classificação de segurança confere a documentos, ou às informações neles contidas, graus de sigilo, conforme legislação específica:

I - A classificação de informações sigilosas é um procedimento previsto para resguardar conteúdo cuja divulgação possa prejudicar, pôr em risco ou comprometer a segurança da sociedade ou do Estado;

II - A atribuição de classificação de segurança a qualquer documento ou informação deverá observar as hipóteses e os graus de sigilo previstos na Lei de Acesso à Informação – LAI, Lei nº 12.527, de 18 de novembro de 2011, e na legislação específica pertinente quanto a outras hipóteses legais de restrição de acesso;

III - A atribuição de classificação de segurança é prerrogativa legal atribuída a certas autoridades com poder decisório;

IV - A atribuição de classificação de segurança depende da análise de conteúdo acerca da informação a ser protegida, que, uma vez restringido seu acesso, somente terão acesso aquelas pessoas que tenham necessidade de conhecê-la, sem prejuízo das atribuições dos agentes públicos autorizados por lei, conforme disposto no § 1°, do art. 25 da LAI;

V - De forma geral, no âmbito do CNMP, serão consideradas de acesso restrito as informações cuja Lei de Acesso a Informação assim preveja, sendo elas:

a) informações classificadas com grau de sigilo (artigo 23 da LAI);

b) informações que componham documento preparatório elaborado para fundamentar tomada de decisão ou ato administrativo (§3° do artigo 6° da LAI);

c) informações que se sujeitem às hipóteses de sigilo previstas em legislação específica (artigo 22 da LAI); e

d) informações pessoais (artigo 31 da LAI).

1) No caso da alínea “a”, deve-se sempre adotar o critério de classificação menos restritivo possível, conforme o § 5° do art. 24 da LAI, considerando: a gravidade do risco ou dano à segurança da sociedade e do estado; o prazo máximo de restrição de acesso ou evento que defina seu termo final.

2) Na hipótese da alínea “b”, ressalvada determinação diversa do usuário responsável pelo expediente, deverão ser classificadas como informações protegidas, do tipo restrito, as notas técnicas, os pareceres, as perícias e outros documentos preparatórios ou informações neles contidas utilizados como fundamento de tomada de decisão ou de ato administrativo, enquanto não editado o ato decisório correspondente.

3) No caso da alínea “d”, as informações de caráter pessoal, que dizem respeito à intimidade, vida privada, honra e imagem, não são públicas e têm seu acesso restrito, independentemente de classificação de sigilo, pelo prazo máximo de 100 anos a contar da sua data de produção.

VI - A restrição de acesso a informações pessoais não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades, conduzido pelo Poder Público, em que o titular das informações for parte ou interessado; ou quando as informações pessoais não classificadas estiverem contidas em conjuntos de documentos necessários à recuperação de fatos históricos de maior relevância;

VII - Será dispensado o consentimento da parte nos casos em que o acesso à informação pessoal for necessário:

a) à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização exclusivamente de tratamento médico;

b) à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo, neste caso, vedada a identificação da pessoa a que a informação se referir;

c) ao cumprimento de decisão judicial;

d) à defesa de direitos humanos de terceiros; e

e) à proteção do interesse público geral e preponderante.

VIII - O setor que detenha a guarda de documento com algum grau de restrição deverá assegurar a não disponibilização ao público até que alcance a ostensividade prevista em lei;

IX - Na hipótese de documento que contenha informações classificadas em diferentes graus de sigilo, será atribuído ao documento o tratamento do grau de sigilo mais elevado;

X - Para dar transparência à classificação das informações que têm acesso temporariamente restrito, o CNMP deve divulgar, anualmente, relação de informações classificadas e desclassificadas em seu site na internet;

XI - A divulgação das informações classificadas com grau de restrição conterá: 1) a natureza do sigilo, seu fundamento e a data da classificação; 2) o período de restrição e a data ou evento que desencadeará a liberação do documento; 3) a autoridade responsável pela restrição;

XII - O CNMP disponibilizará formulário padrão para apresentação de recurso e de pedido de reclassificação, em que a categoria de restrição pode ser alterada para o grau mais ou menos gravoso, bem como para os pedidos de desclassificação de informação secreta ou ultrassecreta e/ou alteração do prazo de sigilo;

XIII - Ao interessado que solicitar acesso à informação não pública, além da obrigação de resguardar o sigilo, será exigida a assinatura de Termo de Compromisso de Manutenção de Sigilo (TCMS), sob pena de responsabilidade penal, civil e administrativa, na forma da lei;

XIV - Ao usuário que tomar conhecimento de documento que contenha informação sigilosa ou restrita ficará obrigado a manter o sigilo, sob pena de responsabilidade penal, civil e administrativa, podendo permitir acesso a terceiros apenas com autorização prévia do responsável pelo setor, salvo disposição diversa em norma específica;

XV - Deverá ser preservado o sigilo em relação à informação classificada por outro órgão ou entidade como ultrassecreta, secreta, reservada, pessoal ou sigilosa, observada a formalidade exigida pelo artigo 28 da Lei n° 12.527, de 18 de novembro de 2011;

XVI - O sigilo da informação classificada deve ser resguardado durante todas as etapas de seu ciclo de vida;

XVII - Os documentos só devem ser desarquivados (eletrônica e fisicamente) mediante solicitação formal à área responsável pela guarda;

XVIII - O documento de natureza sigilosa ou restrita será encaminhado fechado ao respectivo destinatário, com indicação, no envelope, do número de registro nos sistemas eletrônicos, cabendo ao setor do destinatário, se for o caso, a conversão para o formato eletrônico; e

XIX - Os sistemas eletrônicos de documentos devem prever controles de acesso e procedimentos de segurança que garantam a integridade, o uso de controles técnicos e programáticos, assegurando a recuperação rápida em caso de perda devido a sinistro, falha no sistema, contingência, quebra de segurança ou degradação do suporte, mantendo também trilhas de auditoria e de rotinas de cópias de segurança de dados e metadados, conforme dispuser respectiva portaria de implementação.

d.3) Segurança da Informação nas Áreas e Instalações: A Segurança da Informação nas áreas e instalações compreende um conjunto de medidas voltadas a proteger informações sensíveis armazenadas ou em trâmite no espaço físico sob a responsabilidade do CNMP ou no espaço físico onde estejam sendo realizadas atividades de interesse institucional. Esse grupo de medidas engloba ações para estabelecer o fluxo do público interno e externo, controlando o acesso referente às informações de layout de salas e gabinetes, localização de áreas sigilosas ou sensíveis, localização de setores de atendimento ao público e outras.

d.4) Segurança da Informação nos Recursos de Tecnologia da Informação:

• Disposições Gerais

I - Os usuários responsabilizam-se pela utilização de equipamentos, recursos, serviços e sistemas a eles disponibilizados pelo CNMP;

II - Quaisquer incidentes de segurança envolvendo a disponibilidade, a integridade ou a confidencialidade de quaisquer recursos de tecnologia da informação serão tratados em procedimentos administrativos objetivando a identificação dos fatores que o ocasionaram e o restabelecimento das condições operacionais dos recursos envolvidos;

III - O acesso às salas técnicas ou a instalações que contenham equipamentos de uso exclusivo da unidade executiva de tecnologia da informação somente poderá ser realizado mediante autorização e supervisão de servidor desta unidade, salvo no caso de emergências;

IV - A violação de dispositivos deste plano poderá resultar em advertência e/ou na suspensão temporária de privilégios de acesso, após apuração dos fatos mediante procedimento interno da unidade executiva de tecnologia da informação e ratificação da Secretaria-Geral.

V - Eventuais violações que também configurarem infração disciplinar ou crime serão encaminhadas à Secretaria-Geral para as providências cabíveis na esfera disciplinar ou criminal;

VI - Caberá à unidade executiva de tecnologia da informação prover os instrumentos técnicos necessários ao cumprimento das normas e procedimentos estabelecidos neste plano, propondo normativos complementares que não estejam previstos neste plano, mas que sejam necessários para o seu adequado cumprimento; e

VII - Os casos omissos e as dúvidas surgidas na aplicação do presente plano serão dirimidos pela Secretaria-Geral, com o apoio técnico da unidade executiva de tecnologia da informação.

• Dos Recursos de Tecnologia da Informação

Os recursos de tecnologia da informação compõem os equipamentos e infraestrutura de rede de dados em uso institucional pelo CNMP.

São exemplos de recursos de tecnologia da informação:

I - A rede de dados local, seus equipamentos e serviços;

II - A rede de dados sem fio, seus equipamentos e serviços;

III - Os microcomputadores de mesa, portáteis e seus dispositivos periféricos;

IV - Dispositivos móveis institucionais (tablets e smartphones);

V - Os softwares adquiridos e os sistemas desenvolvidos no órgão;

VI - As informações armazenadas, inclusive as mensagens nas caixas de correio eletrônico institucionais, e em tráfego na rede local;

VII - Os canais de comunicação com a internet; e

VIII - Os suprimentos e bens de consumo relacionados à tecnologia da informação.

Os recursos de tecnologia da informação disponíveis no Conselho Nacional do Ministério Público serão utilizados em atividades prioritariamente relacionadas às funções institucionais.

I - O usuário é responsável pelo correto uso dos recursos de tecnologia da informação a ele destinados, devendo zelar pela segurança da informação, comunicando qualquer defeito ou comportamento anormal à unidade executiva de tecnologia da informação;

II - De modo a preservar a segurança da informação nos recursos de tecnologia da informação, o usuário deverá preservar o nível de sigilo da informação a que tiver acesso devido a suas funções institucionais;

III - Somente será permitida a conexão de equipamentos particulares à rede local cabeada em caso de necessidade justificada e mediante solicitação por escrito deferida pela unidade executiva de tecnologia da informação, que realizará as devidas verificações de conformidade de segurança do equipamento;

IV - A configuração de conexão de equipamento particular é de responsabilidade do próprio usuário;

V - A utilização dos equipamentos particulares, seus softwares e serviços, deverão obedecer às regras de utilização e segurança de tecnologia da informação em vigor no CNMP;

VI - É vedada a utilização de mecanismos de compartilhamento de conexão à rede local do CNMP;

VII - É vedada a utilização de qualquer software de testes de segurança, varredura e invasão, quebra de senhas e sistemas, softwares de reengenharia de código, roteadores de conexão, browsers para acesso anônimo em rede do tipo TOR ou outras, bem como qualquer serviço ou software que possa comprometer a segurança ou o vazamento das informações.

• Do Cadastro e Manutenção das Credenciais de Usuários

I - Para a utilização dos recursos de tecnologia da informação do CNMP é necessário o cadastramento do usuário e posterior liberação de acesso;

II - Ao ser credenciado para uso da rede, o usuário será associado a um perfil, que indicará os seus direitos para acesso aos recursos de tecnologia da informação.

III - O usuário será informado sobre a efetivação de seu cadastro, recebendo as senhas iniciais e as instruções básicas para a utilização dos recursos de tecnologia da informação ao qual deverá ter acesso;

IV - A partir do recebimento das senhas iniciais, o usuário passará a ser responsável pela segurança e pelo sigilo de suas contas de acesso e senhas, e por qualquer atividade desenvolvida por meio de seu uso;

V - Sempre que houver mudança de lotação ou desligamento do usuário, a unidade executiva de tecnologia da informação deverá ser informada para que as alterações de acesso aos recursos de tecnologia da informação sejam providenciadas;

VI - Não será concedido perfil em caráter de transição nos casos de transferência entre setores. Caso o usuário necessite de acessos a recursos de sua antiga lotação, estes deverão ter sua disponibilização autorizada pela chefia anterior;

VII - A exclusão do perfil de acesso do usuário implicará na imediata suspensão de todos os acessos e exclusão de caixa de correio eletrônico do usuário;

VIII - Para os casos de colaboradores sem vínculo direto com o CNMP, o setor responsável pela gestão destes deverá encaminhar as solicitações de inclusão, exclusão ou manutenção do cadastro de acesso aos recursos de tecnologia da informação para que a unidade executiva de tecnologia da informação realize os ajustes necessários;

IX - A regra para formação do nome de usuário/e-mail seguirá o padrão definido pela unidade executiva de tecnologia da informação;

X - A identificação do usuário e a senha de acesso são para seu uso exclusivo, ficando terminantemente proibido o compartilhamento; e

XI - Na hipótese de necessidade de utilização de recurso de tecnologia da informação ao qual o usuário não tem acesso, caso o usuário solicitante não se encontre no CNMP, será aceita a solicitação efetuada pelo responsável do setor.

• Dos Critérios Mínimos de Segurança de Senhas de Contas de Usuários

I - As senhas utilizadas no CNMP permitem acesso aos recursos de tecnologia da informação que são disponibilizados conforme a necessidade de cada atividade, e são, obrigatoriamente, de responsabilidade de seus usuários;

II - Todas as senhas devem ser tratadas como informação confidencial, observando-se o prescrito no artigo 116, inciso VIII, e no artigo 132, inciso IX, da Lei 8.112, de 11 de dezembro de 1990, artigo 6º da Lei 12.527/2011 e artigo 325 do Código Penal;

III - A concessão de credenciais de acesso ao usuário deverá observar o critério do privilégio mínimo, onde um usuário não possuirá acesso maior do que aquele necessário para a realização de suas atividades;

IV - A política de senha será definida pela unidade executiva de tecnologia da informação; e

V - As tentativas incorretas de acesso poderão ser armazenadas de forma segura, por um período mínimo de 1(um) ano, para fins de auditoria.

• Das Estações de Trabalho e Dispositivos Móveis Institucionais

I - Estação de trabalho é todo microcomputador de mesa ou portátil adquirido pelo órgão ou particular autorizado em uso na rede de dados do CNMP, bem como seus periféricos;

II - O usuário deverá zelar pelas condições adequadas de instalação dos equipamentos, com atenção especial ao cabeamento do equipamento, que deverá ser mantido em boas condições e manuseado com o devido cuidado. Caso note qualquer anormalidade, deve comunicar o fato à unidade executiva de tecnologia da informação;

III - É vedada a instalação de qualquer software que não tenha sido adquirido ou desenvolvido pelo CNMP, sem a prévia homologação por parte da unidade executiva de tecnologia da informação;

IV - É vedada a cópia dos softwares e sistemas implantados nas estações de trabalho ou dispositivos móveis para uso em outros locais, salvo por autorização em contrário;

V - A configuração e customização do sistema operacional e dos aplicativos instalados nas estações de trabalho e/ou dispositivos móveis institucionais são de responsabilidade da unidade executiva de tecnologia da informação, no que couber, ou por pessoa ou setor por esta autorizada;

VI - Os dados referentes às atividades institucionais deverão obrigatoriamente ser salvos nas unidades de armazenamento de rede, nuvem institucional, ou outro recurso disponibilizado pela unidade executiva de tecnologia da informação;

VII - Não será efetuada cópia de segurança de dados armazenados nas estações de trabalho, dispositivo móvel ou outro local que não disponibilizado pela unidade executiva de tecnologia da informação;

VIII - As cópias de segurança não necessitam de autorização do responsável pelo setor, por se tratar de medidas de segurança inerentes às atividades da unidade executiva de tecnologia da informação;

IX - A cópia e/ou o envio dos dados institucionais para outros meios que não geridos pelo CNMP somente poderão ser efetuados mediante autorização do membro ou responsável do setor, salvo quando solicitado por autoridade competente;

X - A execução de cópias de segurança das unidades de armazenamento de rede será de responsabilidade da unidade executiva de tecnologia da informação;

XI - A periodicidade das cópias de segurança será definida de acordo com os recursos tecnológicos disponíveis;

XII - Os procedimentos e as operações realizadas por intermédio das estações de trabalho e dispositivos móveis institucionais serão de responsabilidade dos usuários que estiverem autenticados;

XIII - Cabe à unidade executiva de tecnologia da informação providenciar a desconexão do equipamento e a sua instalação no local de destino;

XIV - As estações de trabalho e seus periféricos somente poderão ser removidos dos locais de instalação por servidores da área de patrimônio;

• Do acesso à internet

I - O acesso à internet, provido pela rede de dados do CNMP, é prioritariamente destinado ao conteúdo relacionado às funções institucionais;

II - O acesso à internet será oferecido através de níveis de controle, com a definição de perfis de acesso;

III - Todos os acessos à internet serão registrados para eventuais diagnósticos de problemas ou para auditoria nos casos de incidentes de segurança;

IV - Caberá à unidade executiva de tecnologia da informação, em instrumento normativo complementar, o estabelecimento de regras de inspeção automatizada de tráfego visando a mitigar incidentes de segurança e a otimizar a utilização dos canais de acesso à internet;

V - O tráfego criptografado poderá sofrer inspeção como forma de melhor classificar os acessos indevidos e promover auditoria em caso de necessidade ou obrigatoriedade;

VI - Poderá ser concedido acesso à internet a usuário visitante, em caráter temporário, por meio da rede de dados sem fio corporativa do CNMP, priorizando, contudo, o acesso dos usuários vinculados ao CNMP;

VII - O usuário visitante ficará sujeito aos termos deste Plano;

VIII - O acesso a outras redes ou à internet a partir das estações de trabalhos dar-se-á, exclusivamente, por intermédio dos meios autorizados e configurados pela unidade executiva de tecnologia da informação;

IX - A Assessoria de Comunicação Social é o setor responsável pela concessão de acessos para a publicação dos conteúdos nos portais institucionais.

• Da Rede de dados Corporativa

I - Cada setor do CNMP possuirá pasta de rede específica e privativa para suas atividades institucionais, com espaço padrão definido pela unidade executiva de tecnologia da informação;

II - Os conteúdos de pastas que infrinjam leis, especialmente aquelas relacionadas a direitos autorais, ou que não possuam vinculação com as atividades institucionais do CNMP poderão ser removidos pela unidade executiva de tecnologia da informação assim que detectados.

III - Fica vedada a criação, remoção ou transmissão de arquivos que venham a comprometer o desempenho e funcionamento da rede de dados corporativa.

IV - As pastas de troca ou de compartilhamento são de uso geral e não deverão ser utilizadas para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível.

V - Poderá haver limpeza periódica automatizada dos arquivos armazenados nas pastas de troca ou de compartilhamento, para que não haja acúmulo desnecessário de arquivos, ficando facultado à unidade executiva de tecnologia da informação a realização de limpezas extraordinárias.

VI - É vedada a utilização de quaisquer equipamentos e ativos de rede particulares sem autorização prévia da unidade executiva de tecnologia da informação.

VII - Caso autorizada a utilização, equipamentos e ativos de rede particulares deverão observar todas as regras definidas por este Plano a que sejam aplicáveis.

• Rede de Dados Sem Fio Corporativa -WiFi

I - Os usuários poderão utilizar equipamentos particulares conectados à rede de dados sem fio corporativa, utilizando ou não as mesmas credenciais de acesso à rede de dados corporativa;

II - Os equipamentos particulares terão acesso à internet e aos sítios internos do CNMP autorizados;

III - Poderão ser aplicadas restrições de limite de acesso ou de adequações de conformidade, caso o equipamento apresente desconformidade com os padrões mínimos de segurança estabelecidos pela unidade executiva de tecnologia da informação;

IV - Caberá aos usuários a realização das configurações necessárias ao acesso de seus equipamentos particulares à rede de dados sem fio corporativa do CNMP;

V - Os acessos à rede de dados sem fio corporativa por usuários visitantes serão concedidos mediante cadastro para identificação automatizado, ou, na impossibilidade deste, presencial realizado quando da admissão do visitante no CNMP, informando, no mínimo, nome completo, documento de identidade, CPF e e-mail; e

VI - Caberá à unidade executiva de tecnologia da informação propor a regulamentação dos termos da concessão de acesso definidos neste artigo.

• Do Serviço de Correio Eletrônico

I - O serviço de correio eletrônico prestar-se-á exclusivamente ao envio e recebimento de mensagens com conteúdo relacionado às funções institucionais;

II - Cabe à unidade executiva de tecnologia da informação o credenciamento de usuários nos recursos de correio eletrônico institucional;

III - Os setores do CNMP poderão solicitar, com a devida justificativa, a criação de caixas postais institucionais para o setor, temporárias ou de caráter definitivo, que serão criadas de acordo com a viabilidade técnica e orçamentária;

IV - A informação gerada, armazenada, enviada, recebida ou transportada através do sistema de correio eletrônico do CNMP constitui domínio da instituição e deve ser resguardada, considerando-se seu nível de sigilo e criticidade;

V - A gestão adequada dos recursos de armazenamento disponibilizados a uma determinada caixa de correio individual ou corporativa é de responsabilidade do usuário que a possua ou a gerencie;

VI - O tamanho da caixa postal, do anexo e o período de armazenamento das mensagens serão limitados de acordo com os recursos disponíveis;

VII - As mensagens de correio eletrônico poderão ser automaticamente expiradas e eliminadas conforme critérios técnicos definidos pela unidade executiva de tecnologia da informação;

VII - Será realizado controle automatizado do envio e recebimento de mensagens de forma a garantir o correto funcionamento do sistema de correio eletrônico institucional;

VIII - A unidade executiva de tecnologia da informação estabelecerá os critérios de cota, retenção, envio e recebimento de mensagens a serem observados no sistema de correio eletrônico;

IX - Mediante justificativa institucional, poderão ser estabelecidos critérios diferenciados; e

X - É vedado o uso dos recursos do correio eletrônico para a veiculação de mensagens de caráter político-partidário, religioso, publicitário, pessoal, comercial e de “correntes” de qualquer natureza, bem como divulgar informações confidenciais ou privilegiadas, obtidas em razão do cargo e, também, que possam comprometer a honra ou a fama alheia.

• Do Acesso Remoto

I - É facultado aos usuários, mediante a devida autorização, a concessão de acesso remoto seguro(VPN), a partir de ambiente externo às dependências do CNMP, aos recursos de tecnologia da informação;

II - Nesta modalidade de acesso, serão aplicadas as mesmas restrições aplicadas ao usuário quando da utilização dos recursos de tecnologia da informação a ele destinados;

III - Os recursos de tecnologia da informação homologados para acesso remoto, bem como os perfis de usuários autorizados, serão definidos pela unidade executiva de tecnologia da informação e pelas áreas demandantes; e

IV - Poderão ser concedidos acessos para instituições ou indivíduos de forma a viabilizar a realização de serviços remotos no CNMP, assegurados os devidos níveis de segurança da informação.

• Dos serviços em nuvem

Os recursos de tecnologia da informação poderão ser hospedados externamente às dependências do CNMP em ambiente em nuvem;

O disposto neste Plano aplica-se aos recursos de tecnologia da informação hospedados em ambiente de nuvem institucional.

• Do Monitoramento e Auditoria

A unidade executiva de tecnologia da informação poderá implementar medidas que contemplem as seguintes ações:

I - Monitorar, armazenar, analisar conteúdo, filtrar ou impedir o tráfego de rede, de internet e de mensagens de correio eletrônico, por meio de ferramentas automatizadas, conforme critérios por ela definidos e, nos casos excepcionais, pela Secretaria-Geral, com o objetivo de garantir o cumprimento das normas de segurança da informação;

II - Promover auditorias no tráfego de rede e internet ou de mensagens de correio eletrônico, de ofício, ou por solicitação da Secretaria-Geral, para garantir a manutenção da disponibilidade dos recursos de tecnologia da informação;

III - Promover inspeções em recursos de tecnologia da informação do CNMP com o objetivo de verificar a existência de vírus, softwares não licenciados, conteúdo que viole direitos autorais ou propriedade intelectual; e para apurar a conformidade com as regras de segurança da informação;

IV - Suspender serviços de rede, desligar equipamentos ou bloquear acessos, apagar arquivos ou mensagens de correio eletrônico quando tal procedimento se fizer necessário para se restabelecer a operação normal de serviços ou para proteger recursos de tecnologia da informação, devendo ser restabelecida a operação normal assim que cessar a ameaça identificada;

V - Limitar os espaços em áreas de armazenamento destinadas a arquivos ou mensagens de correio eletrônico, de acordo com a disponibilidade de ativos de tecnologia da informação;

VI - Excluir arquivos armazenados em determinadas pastas dos servidores de rede ou correios eletrônicos armazenados a um determinado número de dias, de acordo com critérios previamente estabelecidos a fim de garantir a disponibilidade de ativos de tecnologia da informação e das regras de exclusão definidas neste ou em instrumentos normativos complementares;

VII - Bloquear temporariamente contas de rede, contas de correio eletrônico e outras contas de acesso quando for essencial para garantir ou para preservar a segurança da informação, devendo o acesso ser liberado imediatamente após cessado o evento que deu causa ao bloqueio ou, a qualquer tempo, por determinação da Secretaria-Geral;

VIII - As mídias contendo dados e informações sigilosas devem ser protegidas durante o transporte externo às instalações do CNMP. A proteção será realizada mediante o uso de criptografia;

IX - O uso dos recursos de tecnologia da informação, sempre que possível, deverá gerar informações que possam ser coletadas e transformadas em trilhas de auditoria, de forma que, pela análise ou visualização destas, sejam respondidas questões de autoria e temporalidade;

X - Para fins de verificação do cumprimento das normas de segurança ou por determinação de autoridade competente, a unidade executiva de tecnologia da informação realizará auditoria nas trilhas de uso dos recursos de tecnologia da informação sob sua responsabilidade. As informações provenientes dessas auditorias receberão tratamento sigiloso;

XI - Os equipamentos que forem destinados à doação, considerados inservíveis ou que tenham que sofrer manutenções corretivas em ambientes fora do CNMP, deverão ter seus dados eliminados de forma segura pela unidade executiva de tecnologia da informação; e

XII - As mídias inservíveis contendo dados e informações sigilosos ou sensíveis que por qualquer motivo devam ser destruídas serão eliminadas de forma segura. Deverá ser realizada identificação dos itens que requeiram descarte seguro. O descarte de itens dessa natureza deverá ser registrado em controle com descrição de conteúdo, para permitir a realização de auditorias futuras.

4.2 Segurança Ativa

A segurança ativa é o conjunto de ações de caráter preventivo e proativo destinadas a identificar, avaliar, analisar e neutralizar ameaças dirigidas ao CNMP e a seus integrantes. Serão desenvolvidas a sensibilização, a orientação e a capacitação dos integrantes do CNMP para a proteção da atividade institucional, promovendo a adoção de comportamentos e medidas de segurança relacionadas à contrassabotagem, à contraespionagem e à contrapropaganda.

Tais ações visam a combater as seguintes ameaças:

I - Sabotagem: dano intencional contra instalações ou material, de efeitos físico direto e psicológico indireto, que busca afetar setor e/ou atividade fundamental de uma instituição para a consecução de seus objetivos. Os métodos e processos empregados são extremamente variáveis e dependem das circunstâncias, tendo a imaginação e a criatividade papéis decisivos para a consecução dos objetivos visados.

II - Espionagem: ação planejada que visa à obtenção de dados e conhecimentos de caráter sigiloso de forma a favorecer indevidamente organizações ou indivíduos. A espionagem também pode ser usada para obter informações sigilosas sobre integrantes do CNMP. Caso sejam obtidas, essas informações podem ser utilizadas futuramente para subsidiar um atentado a uma autoridade.

III - Propaganda adversa: emprego planejado da comunicação, no sentido de influenciar grupos sociais pela persuasão, com vistas a obter comportamentos predeterminados que resultem em benefício ao seu patrocinador ou em prejuízo para a Instituição ou indivíduo a quem se destinam.

IV - Outras Ameaças: atividades de qualquer natureza que visam a comprometer ou a superar as medidas de salvaguarda do conhecimento adotadas pelo CNMP.

Em relação à engenharia social, o combate será realizado por meio do incentivo de um comportamento prudente ao tratar de informações relativas à atividade institucional, especialmente aos servidores que lidam diretamente com o público. Esse incentivo ocorrerá por meio de cursos ou palestras, a fim de educar o público interno do CNMP a respeito das principais práticas utilizadas pelos engenheiros sociais, com vistas a que os integrantes da Instituição estejam aptos a antecipar-se a ataques de engenharia social.

5. DISPOSIÇÕES FINAIS

Conforme o parágrafo único do art. 10-E da Portaria CNMP-PRESI nº 160, de 29 de julho de 2014, este Plano de Segurança Institucional será submetido à revisão geral de seu conteúdo a cada dois anos ou, extraordinariamente, quando necessário.