CONSELHO NACIONAL DO MINISTÉRIO PÚBLICO

RELATÓRIO DE AUDITORIA n° 3/2020

AÇÃO DE AUDITORIA: SEGURANÇA DA INFORMAÇÃO

SUMÁRIO EXECUTIVO:

A presente auditoria analisou a suficiência das medidas adotadas para promover a segurança da informação de pessoas, das áreas e instalações, da documentação e dos ativos de tecnologia da informação. O tema foi selecionado para composição do PAINT por meio da metodologia Índice de Significância do Objeto – ISO, na qual o objeto alcançou 1° lugar, de acordo com a percepção dos atores envolvidos na escolha dos temas de auditoria para 2020. Ressalta-se que, pela primeira vez, o tema foi o escopo principal de uma ação da Auditoria Interna.

Foram analisadas, principalmente, a regulamentação e implementação das diretrizes contidas na Política e no Plano de Segurança Institucional, bem como a ocorrência de ação adversa para obtenção indevida de informações, existência de ações de conscientização, condições de armazenamento dos arquivos do órgão e a formalização das políticas específicas de segurança da informação nos ativos de TI.

De modo geral, o CNMP precisa aprimorar o cumprimento do seu Plano de Segurança Institucional, notadamente no que se refere à parte de gestão documental, que ainda não possui uma política definida, nem unidade responsável pelo tema.

I – APRESENTAÇÃO

Em cumprimento ao Plano Anual de Atividades de Auditoria Interna – PAINT 2020, apresenta-se o Relatório de Auditoria sobre Segurança da Informação. Este trabalho contém o resultado da avaliação das medidas adotadas para salvaguardar a segurança das informações que tramitam no CNMP (por meio das pessoas, da documentação, das áreas e instalações e dos recursos de tecnologia da informação), tomando-se como base, em especial, o Plano de Segurança Institucional do CNMP.

Esta ação de auditoria contemplou o controle a posteriori, incluindo fatos e informações dos anos de 2019 e 2020, e controle concomitante, por meio da análise de situações presentes.

O trabalho foi realizado no período de 22/06/2020 a 2/09/2020, sendo executado de acordo com os procedimentos de auditoria geralmente aceitos, na extensão julgada necessária às circunstâncias apresentadas e não houve restrição aos exames.

Em 18/08/2020, foi enviada pelo Sistema Eletrônico de Informações (SEI) a Matriz de Achados de cada unidade (SPR, STI, SA, Secretaria-Geral, Ouvidoria e Presidência), com o objetivo de colher as manifestações dos gestores, bem como identificar as possíveis causas dos achados.

Após a manifestação dos gestores, foi realizada nova análise acerca dos achados para determinar quais seriam objeto de recomendação de auditoria e quais o gestor já havia tomado a devida ciência ou sanado as inconformidades.

II – ESCOPO DO TRABALHO

- Segurança da Informação de Pessoas;
- Segurança da Informação de Áreas e Instalações;
- Segurança da Informação da Documentação;
- Segurança da Informação nos Recursos de TI; e
- Monitoramento de Recomendações Anteriores.

III – METODOLOGIA

Procedimentos de auditoria adotados: Análise documental, questionários, aplicação de checklists, entre outros.

IV – BASE NORMATIVA

- Resolução CNMP n° 171/2017 - Institui a Política Nacional de TI do Ministério Público (PNTI-MP);
- Portaria CNMP-PRESI nº 160/2014 - Institui o CGCE e os Subcomitês a ele vinculados;
- Portaria CNMP-PRESI nº 153/2017 - Regulamenta a Política de Segurança Institucional do CNMP;
- Portaria CNMP-PRESI nº 167/2018 - Institui o Plano de Segurança Institucional do CNMP;

- Portaria CNMP-PRESI nº 190/2018 - Divulga o Plano de Gestão 2019;
- Portaria CNMP-PRESI nº 1/2020 - Divulga o Plano de Gestão 2020;
- Portaria CNMP-SG nº 265/2019 - Aprova o Plano Diretor de Tecnologia da Informação do CNMP para o triênio 2019/2021;
- Portaria CNMP-PRESI n° 169/2012 - Dispõe sobre o acesso à informação e a aplicação da Lei nº 12.527/2011, e da Resolução CNMP nº 89/2012, no âmbito do CNMP;
- Resolução CNMP n° 89/2012 - Regulamenta a Lei de Acesso à Informação (Lei nº 12.527/2011) no âmbito do Ministério Público da União e dos Estados;
- Resolução CNMP n° 158/2017 - Institui o Plano Nacional de Gestão de Documentos e Memória do Ministério Público – PLANAME e seus instrumentos;
- Portaria CNMP-SG nº 136/2020 - Delega perfil de acesso ao Sistema ELO;
- Recomendações para a construção de arquivos. Conselho Nacional de Arquivos – CONARQ, 2000; e
- Classificação, Temporalidade e Destinação de Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública - CONARQ, 2000.

V – RESULTADO DAS ANÁLISES

1. Introdução

Durante o planejamento dos trabalhos, foram elaboradas 4 (quatro) Questões de Auditoria (QA) sobre a Segurança da Informação no CNMP. Cada QA possui itens que foram verificados e testados pela equipe de auditoria. As QA elaboradas foram:

QA 01 – As medidas relacionadas à Segurança da Informação de Pessoas são suficientes para a salvaguarda das informações sensíveis ou sigilosas armazenadas do CNMP?

QA 02 – A segurança da informação na documentação do CNMP garante sua integridade, sigilo, autenticidade, disponibilidade, não repúdio e atualidade?

QA 03 – A segurança da informação de áreas e instalações é suficiente para preservar a integridade, sigilo, autenticidade e disponibilidade das informações armazenadas no CNMP?

QA 04 – A segurança da informação nos recursos de TI é suficiente para preservar a integridade, sigilo, autenticidade e disponibilidade das informações armazenadas no CNMP?

Os achados foram encaminhados por meio das Matrizes de Achados: SPR (SAUDI nº 34/2020 - SEI 0389301), STI (SAUDI nº 35/2020 - SEI 0389306), SA (SAUDI nº 32/2020 - SEI 0389274), SG (SAUDI nº 33/2020 - SEI 0389293), e Ouvidora (SAUDI nº 30/2020 - SEI 0389255), ocasião em que os gestores tiveram a oportunidade de se manifestar. Tais informações constam dos documentos Despacho SPR – SEI 0391061, Despacho STI - SEI 0393888, Despacho SA - SEI 0391998 e Despacho SPR- SEI 0389506, respectivamente. A resposta à Matriz de Achados da Ouvidoria se encontra no próprio documento.

Não constam do presente relatório os achados que foram sanados pelo gestor no decorrer da auditoria. Para os demais, seguem as análises.

2. Universo e Amostragem

O universo da auditoria relacionado aos processos classificados com algum grau de sigilo consta na Lista de Processos Classificados - SEI 0382101. Desses processos, atualmente 97 (noventa e sete) têm classificação de sigilo e todos eles foram testados.

3. Questão de Auditoria 1 - Segurança da Informação de Pessoas

A segurança da informação de pessoas refere-se tanto à proteção de informações sensíveis ou sigilosas dos integrantes do CNMP, quanto à responsabilidade de todos no desempenho de suas funções.

A QA1 pretendeu analisar a suficiência das medidas relacionadas à segurança da informação de pessoas para a salvaguarda das informações sensíveis ou sigilosas armazenadas do CNMP nos seguintes aspectos:

- Ocorrência de ação adversa para obtenção indevida de informações do CNMP;
- Medidas utilizadas para verificar e monitorar as ações de prestadores de serviços;
- Promoção da cultura comportamental de combate a ataques de engenharia social;
- Representações à Comissão de Ética sobre as condutas que envolvam a segurança e o sigilo das informações; e
- Assinatura de termo de conhecimento do Código de Ética do CNMP.

O Plano de Segurança Institucional do Conselho Nacional do Ministério Público (PSI), normatizado pela Portaria CNMP-PRESI nº 167/2018, Anexo II, dispõe, no item 4.1, d.1, I, que um dos objetivos da segurança da informação de pessoas é “Detectar, prevenir e gerenciar as infiltrações, recrutamentos e outras ações adversas de obtenção indevida de informações”.

A fim de verificar o cumprimento desse objetivo, foram encaminhadas a SAUDI nº 18/2020 - SEI 0376687 à Secretaria de Gestão de Pessoas – SGP e a SAUDI nº 23/2020 - SEI 0377145 à Corregedoria Nacional. Em resposta, as duas unidades informaram que, até o momento, não foram detectadas ações adversas para obtenção indevida de informações, conforme Despacho SGP – SEI 0376975 e Memorando nº 10/2020/CGAB/CN - SEI 0380550.

Na mesma linha, em resposta à SAUDI nº 20/2020 - SEI nº 0376700, a Secretaria de Tecnologia da Informação - STI informou (Despacho STI – SEI 0379379) que, de 1/7/2019 a 30/6/2020, foram observadas tentativas de ataque à rede do CNMP, contudo nenhuma delas logrou êxito. Além disso, declarou que a unidade adota medidas proativas ou sob demanda para melhorar a segurança da informação nos ativos de TI.

O mesmo normativo, no item 4.1, d.1, III, prevê o objetivo de "Verificar e monitorar as ações de prestadores de serviços à Instituição".

Nesse aspecto, é possível observar que os contratos firmados pelo CNMP com previsão de mão de obra possuem cláusulas padrões que abordam o uso de uniformes e identificações, a observância das normas de segurança do órgão, o sigilo de informações, a proibição de reproduzir, divulgar ou utilizar informações sem autorização e a ciência e submissão ao Código de Ética do CNMP.

A fim de verificar se já houve aplicação de penalidades a empresas contratadas em razão do descumprimento de tais cláusulas, a SA informou, em resposta à SAUDI nº 17/2020 - SEI 0376662, por meio do Despacho SA – SEI 0377721, que o Núcleo de Contratos não tem conhecimento de nenhum processo de penalidade instaurado para apuração de descumprimento de cláusulas que disponham sobre o sigilo das informações a que os terceirizados tenham acesso.

A SAUDI nº 20/2020 - SEI 0376700, questionou à Secretaria de Tecnologia da Informação, dentre outros pontos, se há medidas para verificação e monitoramento das ações dos prestadores de serviços, como acesso aos sistemas, correio eletrônico, navegação na internet, ataques de engenharia social. Por meio do Despacho STI – SEI 0379379, a unidade informou que "Todos os usuários que interagem com os ativos de TI são monitorados pelos controles de segurança implementados, de forma igual, independentemente de sua natureza".

Já o item 4.1, d.1, IV do PSI, trata do objetivo de "Promover a cultura comportamental de combate a ataques de engenharia social". A SAUDI nº 20/2020 - SEI 0376700 também questionou à STI as medidas empregadas para promover a cultura comportamental de combate a ataques de engenharia social. A unidade respondeu (Despacho STI – SEI 0379379 que faz a conscientização por meio da divulgação de notícias na intranet e citou como exemplo as notícias "STI alerta para falsas mensagens de correio eletrônico", "Usuários do sistema ELO devem ficar atentos a e-mails recebidos" e "Saiba como proteger sua conta no Whatsapp e no Telegram", todas publicadas em 2019.

O Código de Ética do CNMP, Portaria CNMP-PRESI nº 44/2018, em seu artigo 6º, inciso XXIII, dispõe que:

> Art. 6º É vedado ao servidor do CNMP: (...)
>
> XXIII – dar conhecimento de atos, documentos, dados ou assuntos internos, mesmo que não sigiloso, a quem deles não deva ter ciência ou não tenha atribuições para neles intervir, resguardado o direito à informação, nos termos da lei.

Já em seu inciso XVIII, há a proibição de:

> XVIII – assumir compromissos, prestar declarações ou divulgar informações, em nome da Instituição, sem autorização.

Considerando as competências da Comissão de Ética previstas no art. 8º, foi encaminhada a SAUDI nº 19/2020 - SEI 0376697 questionando eventual recebimento de representações. Em resposta, por meio do Despacho CE-CNMP – SEI 0377911, a Comissão informou que não houve, até o momento, nenhuma representação pela infração aos dispositivos citados do Código de Ética.

O Código de Ética dispõe, ainda, no art. 11 que:

> Os atuais servidores do CNMP, bem como aqueles que vierem a tomar posse em cargo de sua estrutura, assinarão termo de conhecimento das disposições deste Código de Ética, firmando compromisso de observá-lo no desempenho de suas atribuições.

Para dar cumprimento a este dispositivo, foi criado no SEI o documento "Código de Ética – Termo de Conhecimento". No dia 5/5/2020, foi publicada notícia na Intranet sob o título "Servidores devem assinar termo de conhecimento do Código de Ética". Além da divulgação pela Intranet, a Secretaria de Gestão de Pessoas - SGP enviou, em 27/4/2020, o documento por e-mail aos servidores.

Até o dia 24/7/2020, verificou-se que 242 (duzentos e quarenta e dois) documentos desta natureza foram expedidos e assinados, o que representa 88% (oitenta e oito por cento) dos servidores do CNMP.

Diante do exposto, as medidas adotadas até o momento foram suficientes para preservar a segurança da informação de pessoas e, assim, proteger informações sensíveis ou sigilosas.

4. Questão de Auditoria 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 do CNMP, em todas as suas fases: produção e recepção; organização; uso e disseminação; e destinação.

A QA2 teve o objetivo de verificar a suficiência das medidas destinadas a garantir a integridade, o sigilo, a autenticidade, a disponibilidade, o não repúdio e a atualidade das informações no que se refere à documentação do CNMP.

Para tanto, foram adotados como parâmetros principalmente o Plano de Segurança Institucional - PSI (Portaria CNMP-PRESI n° 167/2018) e a Política de Segurança Institucional (Portaria CNMP-PRESI n° 153/2017), mas também foram adotadas a Resolução CNMP n° 158/2017, a Resolução CNMP n° 89/2012 e a

Portaria CNMP-PRESI n° 169/2012, por serem normas correlatas. Ademais, a questão discorreu sobre os seguintes requisitos:

- Existência de protocolos de segurança para os documentos eletrônicos ostensivos e sigilosos;
- Ocorrência de violação da informação de documentos com grau de restrição e, em caso positivo, quais medidas foram adotadas;
- Existência de Plano/Código de Classificação e Tabela de Temporalidade e Destinação de Documentos;
- Existência de Política de Gestão de Arquivo Documental;
- Aderência da classificação de documentos e informações à LAI e aos normativos internos;
- Divulgação da relação de informações classificadas com grau de sigilo no Portal do CNMP; e
- Existência de ações de conscientização, educação e treinamento em segurança da informação da documentação.

Para chegar às conclusões relatadas, foram averiguadas as respostas às SAUDIs nº 20/2020 - SEI 0376708, nº 21/2020 - SEI 0076729, n° 30/2020 - SEI 0389255, n° 33/2020 - SEI 0389293 e n° 34/2020 - 0389301, o Portal do CNMP, a Intranet, o Serviço de Informações ao Cidadão (SIC) e o SEI.

De modo geral, observou-se que o CNMP dispõe de medidas adequadas e razoáveis para garantir a segurança da informação na documentação, a exemplo das regras e protocolos de acesso aos arquivos físicos relatados na QA3 e da definição de perfis e níveis de acesso aos principais sistemas da Casa (SEI e ELO).

Ademais, no Despacho 0379969, a Secretaria de Tecnologia da Informação (STI) ressaltou que, em ambos os sistemas, as informações trafegam criptografadas por meio do protocolo https (http seguro), existe um sistema gerenciador de bancos de dados para garantir a integridade, há dois servidores (computadores) potentes trabalhando com balanceamento de carga para assegurar a disponibilidade e são utilizadas assinaturas digitais com a finalidade de garantir a autenticidade e o não repúdio.

Não obstante, também foram constatadas algumas inconsistências que aumentam o potencial de riscos relacionados, sobretudo, à violação aos aspectos de sigilo, disponibilidade, atualidade e transparência das informações.

4.1 Informação: Risco de vazamento de informação sigilosa

De acordo com o que consta do Processo 0.00.000.001651/2011-88, digitalizado no Processo SEI 19.00.1000.0001676/2019-08, no ano de 2010, a então Conselheira Cláudia Chagas deferiu sigilo ao Procedimento de Controle Administrativo (PCA) nº 0.00.001964/2010-55. No entanto, a identidade do requerente vazou no site do CNMP, devido a falhas nos procedimentos operacionais de trânsito e guarda do PCA.

Diante da constatação, a Conselheira requereu regulamentação urgente acerca dos procedimentos adotados no que tange aos sigilos decretados. Para o atendimento da demanda, em 2011, foi elaborada minuta de portaria regulamentando o tema, mas nos autos não consta a concretização da norma.

Nada obstante, nesse interregno, foram publicadas a Resolução CNMP n° 89/2012 e a Portaria CNMP-PRESI n° 169/2012, que regulamentaram a Lei de Acesso à Informação- LAI (Lei n° 12.527/2011) e, embora abordem o tema do sigilo das informações, não regulamentam tais procedimentos.

Todavia, no Parecer 01/2016-COPF/SPR, o Analista de Arquivologia da Secretaria Processual (SPR) discorre sobre o tema da classificação das informações e aponta diversas recomendações, dentre elas, a necessidade de melhorias na Portaria CNNMP-PRESI n° 169/2012 para que ela possa atender a todos os aspectos obrigatórios exigidos pela LAI, inclusive os procedimentos a serem aditados nas informações sigilosas.

Em decorrência desse trabalho, atualmente o Processo SEI 19.00.1000.0001676/2019-08 encontra-se na Ouvidoria Nacional com minuta de portaria de atualização da Portaria CNMP-PRESI 169/2012 e sua Seção IV regulamenta o "Trânsito e da Guarda das Informações Sigilosas".

Com essa regulamentação, criam-se controles mais efetivos para que seja preservada a segurança dos documentos sigilosos e não ocorra vazamento de informação como aconteceu em 2010.

4.2 Constatação: Processo de classificação das informações não aderente à Portaria CNMP-PRESI nº 169/2012 e à Lei nº 12.527/2011 - LAI

Análise: Como dito, a Lei n° 12.527/2011- LAI, foi regulamentada no âmbito do CNMP pela Resolução n° 89/2012 e pela Portaria CNMP-PRESI n° 169/2012. De acordo com o previsto no art. 3° da Resolução, o CNMP deverá assegurar:

> I – gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação;
>
> II – proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e
>
> III – proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.

Ainda, o art. 17 da aludida Resolução atribui a competência de regulamentar os procedimentos de classificação de informações, em especial quanto aos graus e prazos de sigilo, ao Presidente do CNMP. Nessa seara, a regulamentação ocorreu por meio da Portaria CNMP-PRESI n° 169/2012, que, em seu art. 6º, preceitua:

> Art. 6° Compete ao Presidente, Corregedor, Conselheiros e Secretário-Geral classificar e controlar o acesso a informações sigilosas por eles produzidas ou custodiadas, assegurando a devida proteção, observando o disposto no Capítulo IV da Lei nº 12.527 quanto às restrições de acesso à informação, em especial quanto aos graus e prazos de sigilo.

Para verificar o cumprimento do dispositivo, solicitou-se à SPR, por meio da SAUDI n° 21/2020 - SEI 0376729, lista com os números de todos os processos classificados como restritos e sigilosos, e os responsáveis pelas respectivas classificações, no período de 01/07/2019 a 30/06/2020. Em resposta, a SPR encaminhou a Planilha SEI 0382101 com os números de 3.036 (três mil e trinta e seis) documentos, dentre os quais, atualmente 97 (noventa e sete) estão com grau de sigilo. Diante do universo, a Auditoria selecionou esses 97 (noventa e sete) processos para análise e constatou que foram analistas e técnicos administrativos os responsáveis por colocar sigilo nos documentos.

Ademais, em teste realizado no SEI, no tipo de processo "Administração – Apuração de Penalidade – Apuração de Descumprimento Contratual", verificou-se que qualquer usuário, independentemente de seu perfil de acesso, pode classificar uma informação como sigilosa, o que aumenta o risco de prejudicar a transparência e a disponibilidade da informação.

Portanto essas constatações não estão aderentes com o mandamento do art. 6° da Portaria CNMP-PRESI n° 169/2012.

Em resposta à matriz de achados, SAUDI n° 34/2020 - SEI 0389301, a SPR manifestou-se nos seguintes termos:

> Existem diferentes tipos de sigilo, além daqueles elencados na LAI. A arquitetura de criação de documentos no SEI permite a atribuição de sigilo a processos, conforme sua natureza, que pode levar em consideração diversos fatores. O sistema em si, só controla, como deve ser, que ao processo que tenha sido atribuído sigilo, permaneça como tal, sigiloso. A verificação acerca da atribuição de sigilo, se foi autoridade competente ou não, diz respeito ao rito interno do próprio objeto do procedimento, que vai além do escopo de controle do sistema, uma vez que é responsabilidade daqueles envolvidos identificar ilegalidade, e se está conforme os parâmetros legais apontados nesta auditoria.

E continuou:

> O controle prévio ou posterior sobre a atribuição de sigilo em um processo do SEI deve ser realizado internamento no procedimento. Por dois motivos, a nosso ver. Um primeiro de proteção ao devido processo legal, e outro de arquitetura do sistema, que parte do pressuposto de gestão de processos por unidade, e não por pessoas. No momento em que é atribuído sigilo, automaticamente essa arquitetura muda e passa a ser controlado pessoa a pessoa. Estas devem levantar qualquer vício quanto possível ilegalidade de atribuição no âmbito do próprio processo.

Convém ressaltar, contudo, que, no Parecer 0192164 do Processo SEI 19.00.1000.0001676/2019-08, o Analista de Arquivologia da SPR destaca a necessidade de atualização das autoridades competentes pela atribuição de grau de sigilo e a definição de todas as informações passíveis de classificação.

O atendimento da necessidade está previsto na minuta de portaria anexada ao Processo supracitado, a qual, em seu art. 34, define os seguintes regramentos:

> Art. 34. A classificação de informação é de competência:
>
> I – no grau de sigilo ultrassecreto: do Presidente e do Plenário;
>
> II – no grau de sigilo secreto: do Presidente, do Plenário, do Corregedor Nacional, do Ouvidor, dos Conselheiros e do Secretário-Geral;
>
> III – no grau de sigilo reservado: das autoridades referidas nos incisos I e II e dos que exerçam o cargo de Secretário no CNMP.
>
> **§ 1º Fica vedada a delegação da competência de classificação nos graus de sigilo ultrassecreto e secreto.**
>
> § 2º O Presidente e o Plenário poderão delegar a competência para classificação no grau de sigilo reservado a agente público que exerça função de direção, comando ou chefia, sendo vedada a subdelegação da competência.
>
> § 3º Os agentes públicos delegados para classificar informação com grau de sigilo reservado deverão dar ciência do ato de classificação à autoridade delegante, no prazo de 90 (noventa) dias.
>
> **§ 4º A classificação em grau de sigilo deve ser realizada preferencialmente no momento em que a informação for gerada ou acautelada no CNMP.** (Grifos nossos)

Adiciona-se o art. 38 da minuta em comento, o qual preceitua:

> Art. 38. É de responsabilidade do servidor que produziu ou recebeu a informação passível de classificação dar ciência à chefia imediata, que deverá encaminhá-la à autoridade classificadora competente.

Alerta-se, portanto, que a definição das autoridades responsáveis por colocar sigilo nos documentos é imprescindível, porém não é suficiente, pois há a necessidade de que os sistemas eletrônicos da Casa reflitam essa nova regulamentação, permitindo apenas às autoridades com perfil elencados no art. 34 da minuta da portaria a possibilidade de apor sigilo nos documentos.

Do contrário, corre-se o risco de o referido artigo, bem como o art. 38, caso a portaria seja aprovada, tornarem-se meras normas editadas, sem aplicabilidade na prática, ferindo, como dito na resposta à matriz de achados, o devido processo legal.

Nesse contexto, após reunião de encerramento da auditoria, a Secretária Processual encaminhou manifestação do gestor (Despacho SPR 0399029) informando que aguarda a publicação de normativo que visa atualizar a Portaria CNMP-PRESI nº 169/2012, atualmente sob revisão da Ouvidoria Nacional, para realizar as alterações permitidas pelo Sistema SEI.

Recomendação: Recomenda-se à Secretaria Processual que promova a adequação das regras de aposição de sigilo no sistema SEI ou da legislação vigente.

4.3 Constatação: Publicação incompleta das informações classificadas com grau de sigilo no Portal da Transparência

Análise: Consoante o § 3° do art. 25 da Resolução 89/2012, "O CNMP e cada Ministério Público manterão extrato com a lista de informações classificadas, acompanhadas **da data, do grau de sigilo e dos fundamentos da classificação**". (Grifo nosso)

Na mesma esteira, o Plano de Segurança Institucional - PSI (Portaria CNMP-PRESI n° 167/2018) determina, no item 4.1, d.2.1, XI, que "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**". (Grifo nosso)

Preliminarmente, convém ressaltar que o PSI é mais abrangente que a Resolução n° 89/2012, pois contempla, os pontos 2 e 3, não previstos na Resolução. Nesse espírito, foram averiguados os extratos de informações classificadas com grau de sigilo referentes aos anos de 2015 a 2019, disponibilizadas no Portal da Transparência – Publicação Anual do SIC.

Constatou-se que, conforme declarações de 2019 e 2018, não houve registro de informações sigilosas nesses dois anos. Já em 2017, 2016 e 2015 existiram 36 (trinta e seis), 51 (cinquenta e um) e 47 (quarenta e sete) processos com grau de sigilo, respectivamente. Todavia, o rol das informações classificadas se constitui de tabelas do Excel com campos que não contemplam o disposto no § 3°, art. 25 da Resolução 89/2019 e/ou ao constante do item 4.1, d.2.1, XI, do PSI, como se verifica nos campos do extrato abaixo, relativos à planilha do ano de 2017.

Número do Procedimento	Sistema de Origem	Data de Distribuição	Classe Processual	Fase Processual

Constatou-se, ainda, que os extratos não contemplam nenhuma informação com grau de sigilo relativas aos processos do SEI, mas apenas aos processos do Sistema ELO e do CNMP/METAFRAME.

Portanto, esse cenário não atende ao disposto nos normativos que regem a matéria no CNMP e prejudica os princípios da transparência, da disponibilidade e da atualidade da informação.

Importa ressaltar que a minuta de portaria que visa atualizar a Portaria CNMP-PRESI n° 169/2012 também abordou o tema em seu art. 54, § 2°. Porém, destaca-se o fato de continuar sendo mais restritiva que o PSI, uma vez que não contempla a necessidade de divulgar a autoridade responsável pela classificação.

> Art. 54, § 2º Compete ao representante da Ouvidoria Nacional do Ministério Público:
>
> I – avaliar e monitorar a implementação do disposto nesta Portaria;
>
> II – orientar as unidades do CNMP no que se refere ao cumprimento desta Portaria;
>
> **III – publicar, anualmente, até o dia 1º de junho, o rol das informações desclassificadas, bem como o rol das informações classificadas em cada grau de sigilo, nos últimos 12 (doze) meses, devendo conter:**
>
> **a) categoria na qual se enquadra a informação;**
>
> **b) indicação de dispositivo legal que fundamenta a classificação; e**
>
> **c) data da produção, data da classificação e prazo da classificação.**
>
> IV – publicar, anualmente, até o dia 1° de junho, relatório estatístico contendo a quantidade de pedidos de acesso à informação recebidos, atendidos e indeferidos, discriminados por unidade, bem como informações genéricas sobre os solicitantes. (Grifo nosso).

Em resposta à matriz de achados, a Ouvidoria Nacional informou que o rol de informações está desatualizado basicamente por dois motivos:

> - Alteração da gestão da Ouvidoria Nacional (informações acostadas em gestões anteriores da Ouvidoria Nacional); e
>
> - Ausência, no âmbito do CNMP, de ato regulamentando a LAI. A falta desta regulamentação pode ser o fator que impede a disponibilização das informações para a publicação anual do SIC, não existindo, portanto, rotinas e fluxos de trabalho para que as informações sejam corretamente classificadas (em análise – Ouvidoria e Presidência – de portaria dispondo sobre o tema – vide: processo sei 1676/2019-08)

Ademais, acrescentou:

> É possível que as informações acostadas relativas aos anos de 2015 a 2018 devam ser revistas e eventualmente republicadas. Isso porque pode ter ocorrido possível confusão a respeito da natureza das informações, se sigilosas ou pessoais. Em determinados processos da área fim, partes solicitam o sigilo de seus dados pessoais, o que pode ter ensejado a inclusão destes procedimentos como sigilosos. Para tanto, necessário o envolvimento das áreas do CNMP

> com acesso a essas informações e atribuição para revisão (Presidência, Secretaria Processual, Corregedoria Nacional – rol sugestivo).

A unidade informou ainda que, além da minuta de portaria, existe no Plano de Gestão 2020 a iniciativa em andamento "PG_20_OUV_015_ Revisão dos atos normativos relacionados à aplicação da Lei de Acesso à Informação no âmbito do CNMP".

Recomendação a: Recomenda-se à Ouvidoria Nacional que os extratos das informações sobre classificação e desclassificação de sigilo publicados no Portal da Transparência do CNMP contemplem todos os requisitos exigidos pelo item 4.1, d.2.1, XI, do Plano de Segurança Institucional.

Recomendação b: Recomenda-se à Ouvidoria Nacional que avalie quanto à inclusão, no rol das informações sigilosas divulgadas no Portal da Transparência, dos processos com classificação de sigilo no SEI, em atendimento ao item 4.1, d.2.1, XI, do Plano de Segurança Institucional.

4.4 Constatação: Ausência de Plano/Código de Classificação e Tabela de Temporalidade e Destinação de Documentos do CNMP

Análise: O Plano de Segurança Institucional - PSI, no item 4.1, d.2.1, II, dispõe que a gestão de documentos no CNMP se dará com base no Plano de Classificação e Tabela de Temporalidade e Destinação do Documentos do Órgão, conforme se verifica:

> 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;

Preliminarmente, convém registrar as definições de Código de Classificação e de Tabela de Temporalidade e Destinação de Documentos. Para tanto, utilizam-se os conceitos constantes do manual "Classificação, Temporalidade e Destinação De Documentos de Arquivo Relativos às Atividades-Meio da Administração Pública", páginas, 9 e 43, respectivamente, publicado pelo CONARQ.

> O código de classificação de documentos de arquivo é um instrumento de trabalho utilizado para classificar todo e qualquer documento produzido ou recebido por um órgão no exercício de suas funções e atividades. A classificação por assuntos é utilizada com o objetivo de agrupar os documentos sob um mesmo tema, como forma de agilizar sua recuperação e facilitar as tarefas arquivísticas relacionadas com a avaliação, seleção, eliminação, transferência, recolhimento e acesso a esses documentos, uma vez que o trabalho arquivístico é realizado com base no conteúdo do documento, o qual reflete a atividade que o gerou e determina o uso da informação nele contida. A classificação define, portanto, a organização física dos documentos arquivados, constituindo-se em referencial básico para sua recuperação.
>
> (...)
>
> A tabela de temporalidade é um instrumento arquivístico resultante de avaliação, que tem por objetivos definir prazos de guarda e destinação de documentos, com vista a garantir o acesso à informação a quantos dela necessitem. Sua estrutura básica deve necessariamente contemplar os conjuntos documentais produzidos e recebidos por uma instituição no exercício de suas atividades, os prazos de guarda nas fases corrente e intermediária, a destinação final – eliminação ou guarda permanente –, além de um campo para observações necessárias à sua compreensão e aplicação.

De posse desses conceitos e após averiguação na Intranet, na aba Atos e Normas, a equipe de auditoria constatou que o CNMP ainda não instituiu tais instrumentos de gestão documental.

Para ratificar a constatação, também foram analisadas 8 (oito) atas do Grupo de Trabalho Gestão Documental e Tabela de Temporalidade do Comitê Gestor do Plano Nacional de Gestão de Documentos e Memória do Ministério Público (COPLANAME). Na ata da sétima reunião, realizada em 11/10/2019, há a informação de que já fora elaborada uma minuta de resolução disciplinando o Código de Classificação e Tabela de Temporalidade e Destinação de Documentos da área-meio do Ministério Público, a qual está pendente de aprovação pelo Plenário.

Impende destacar, todavia, que as atribuições do COPLANAME estão voltadas para as Unidades e Ramos do Ministério Público brasileiro, conforme art. 3° da Resolução n° 158/2017.

> Art. 3º O Comitê Gestor do Plano Nacional de Gestão de Documentos e Memória do Ministério Público – COPLANAME, órgão colegiado, vinculado à Presidência do Conselho Nacional do Ministério Público, tem por finalidade definir a Política de Gestão Documental e de Memória do Ministério Público, bem como exercer orientação normativa, visando à gestão documental e à implementação de memoriais nas unidades do Ministério Público.

Diante desse cenário, a equipe de auditoria reuniu-se, no dia 28/09/2020, por meio do Teams, com a Secretaria Processual e um representante do COPLANAME para entender se a resolução a ser aprovada também disciplinaria o tema no âmbito do CNMP e se já havia trabalhos em andamento relativos aos documentos da área-fim.

Sobre o primeiro ponto, foi informado que a resolução irá contemplar o CNMP. Já quanto ao Código de Classificação e Temporalidade e Destinação de Documentos da área-fim, destacou-se que

o COPLANAME está desenvolvendo uma minuta, porém, não abrangerá o CNMP. Mas, posteriormente, será instituído um grupo de trabalho com a finalidade de elaborar o documento para o Órgão.

Por fim, sobre o Código de Classificação e Tabela de Temporalidade da área-meio, convém ressaltar que a proposta de resolução que o institui consta do Processo SEI 19.00.2018.0009700/2019-17. Conforme justificativa da proposição, seu objetivo é "criar o Plano de Classificação de Documentos (PCD) e a Tabela de Temporalidade e Destinação de Documentos do Ministério Público (TTD) - Área Meio". Portanto, não cita, explicitamente, o CNMP em seu escopo de abrangência. A mesma conclusão pode ser extraída dos 7 (sete) artigos que a norma contempla. Em todos eles, não há menção ao fato que a norma também será aplicada ao CNMP.

Além disso, observou-se que a proposta foi enviada a todos os chefes das unidades e ramos do Ministério Público, mas não há registo de envio à manifestação das chefias do CNMP, como por exemplo, o Secretário-Geral.

Diante do todo exposto, verifica-se a ausência de cumprimento do dispositivo 4.1. d.2.1, II do Plano de Segurança Institucional.

Recomendação: Recomenda-se à Secretaria-Geral que envide esforços no sentido de promover a elaboração e publicação do Plano/Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos do CNMP, abrangendo tanto a área-meio quanto à área fim da Instituição.

4.5 Constatação: Falta de formalização da Política de Gestão de Arquivo Documental do CNMP

Análise: De acordo com o item 4.1, d.2.1, III, do Plano de Segurança Institucional - PSI, o CNMP deve definir sua política de gestão de arquivo documental:

> 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.

Em consulta realizada na Intranet, na aba "Atos e Normas", não foi encontrado nenhum ato específico normatizando e institucionalizando a matéria. Adicionalmente, a SPR, no Despacho 0379676, informou não haver ação em andamento no CNMP com o objetivo de institucionalizar essa Política. E, na resposta à matriz de achados, SAUDI n° 33/2020 - SEI 0389293, a SPR sugeriu uma estrutura mínima para a Política, nos seguintes termos:

> (...) A declaração pode incluir as linhas gerais do programa de gestão, bem como os procedimentos necessários para que essas intenções sejam alcançadas. Deve também ser comunicada e implementada em todos os níveis dos órgãos e entidades. No entanto, a declaração por si só não garante uma boa gestão arquivística de documentos. Para a política ser bem-sucedida, são fundamentais o apoio da direção superior e a alocação dos recursos necessários para sua implementação. A viabilidade dessa política passa necessariamente pelo patrocínio da direção hierárquica superior.
>
> A política de gestão arquivística de documentos deve explicitar as responsabilidades e designar as autoridades envolvidas no programa de gestão (unidades e servidores), de forma que, por exemplo, quando for identificada a necessidade de orientar sobre a produção, capturar, armazenamento, digitalização e recuperação de documentos, esteja claro qual é a unidade responsável por essas ações.

Destaca-se que a falta de uma política institucionalizada, com a definição de responsabilidades e atribuições das unidades, gestores e demais colaboradores, coloca em risco a integridade, o sigilo, a autenticidade e a disponibilidade dos documentos produzidos e mantidos pelo Órgão.

Em decorrência disso, observou-se, por exemplo, uma inadequação do sistema de climatização nas salas de arquivo. As análises utilizadas para essa constatação tiveram como base o documento "Recomendações para a construção de arquivos" elaborado pelo Conselho Nacional de Arquivos – CONARQ, em 2000. Cabe salientar que o CNMP não possui normativo específico sobre o tema.

No item 8.1, o documento versa sobre temperatura e umidade relativa do ar. A umidade relativa, se em níveis muito baixos (abaixo de 40%) causa danos ao papel e, se muito alta (acima de 65%) torna o ambiente suscetível à proliferação de micro-organismos. Portanto, a faixa segura recomendada é entre 45 e 55%. Quanto à temperatura, a publicação indica que 20º é o ideal para documentos.

O documento diz ainda que "O sistema de climatização deve ser independente para as áreas de depósitos, pois devem atender às necessidades de preservação dos documentos ali armazenados e manter condições estáveis, exigindo que os equipamentos funcionem sem interrupção".

Conclui afirmando que um sistema de ar-condicionado ideal possui controle de temperatura, de umidade e sistema de filtragem dos agentes poluentes. Além disso, deve ser mantido em funcionamento durante as 24 (vinte e quatro) horas do dia.

A SAUDI nº 17/2020 - SEI 0376662 solicitou à SA informações sobre controle de temperatura e umidade nos ambientes em que são armazenados processos e outros documentos físicos e questionou se o sistema de ar-condicionado possui mecanismo de filtragem de ar.

Segundo Despacho COENG – SEI 0377382 e e-mail datado de 30/7/2020, a sala de arquivo da COOFIN e os arquivos da Corregedoria localizados nos pavimentos G1 e G2 não possuem sistema de climatização.

Já o arquivo da SGP e o arquivo da SPR localizados na cobertura possuem condicionamento de ar por meio do sistema central do edifício. Portanto, não há controle de temperatura nas salas, apenas o ajuste da

temperatura do ar-condicionado central, por ala. A unidade destaca que o referido sistema não funciona nos horários fora do expediente normal do prédio, como no período noturno, finais de semana e feriados.

Em resposta à matriz de achados encaminhada à SA por meio da SAUDI n° 32/2020 - SEI 0389274, a unidade também defendeu a necessidade de normatização de uma política interna sobre os requisitos básicos para ambientes destinados a guarda de documentos que aborde temas como controle de acesso; monitoramento por vídeo; detecção, alarme e combate a incêndio, adequado ao material armazenado; umidade; temperatura; iluminação; parâmetros de acessibilidade; dentre outros. Sugere, ainda:

> a unificação dos vários arquivos do CNMP em um único local, fora da área dos escritórios, de modo a reduzir os custos de investimento para implantação das soluções, bem como o custo permanente de manutenção, além de liberar áreas de escritório para outros fins, como a expansão de área de escritório.

Na reunião de encerramento, questionado sobre a viabilidade e a pertinência de promover a climatização individual das salas de arquivo do CNMP, enquanto não estiver definida a Política de Gestão Documental e a unidade responsável pelos procedimentos, o Secretário de Administração manifestou-se no sentido de que é preciso aguardar a elaboração da Política de Gestão de Arquivos antes de realizar qualquer investimento nos atuais arquivos, conforme Despacho SEI 0398829.

Outra constatação diretamente relacionada à falta da Política diz respeito à ausência de conscientização, educação e treinamento em segurança da informação da documentação do CNMP, o que vai de encontro aos objetivos traçados no Plano de Segurança Institucional, quando este afirma que o CNMP deve promover a disseminação da cultura de segurança institucional (art. 2°, IV), e que o Órgão "desenvolverá programa de capacitação e treinamento dos seus integrantes, para garantir a implementação e a execução das normas, dos procedimentos e das técnicas de segurança" (art. 18).

Para essa constatação, também foram realizadas pesquisas na Intranet e no Portal do CNMP, ocasião em que não foram encontradas matérias relativas à promoção de ações no sentido de capacitação e conscientização dos servidores acerca da segurança da informação na documentação. Ainda, foram analisados os planos de gestão de 2019 e de 2020, mas também não há ações nesse sentido.

Em resposta à matriz de achados, SAUDI n° 33/2020 - SEI 0389293, a SPR se manifestou nos seguintes termos:

> Partindo do pressuposto que segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio (ISO 17799, 0.1). E que a informação pode existir em diversas formas, podendo ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas, não se restringindo somente a documentos arquivísticos. A capacitação em segurança da informação da documentação passa por uma avaliação de risco que deve ser analisada em conjunto por toda organização, levando em consideração diversos outros quesitos e unidades, tais como proteção de dados, registros organizacionais, e a própria política de segurança da informação e da classificação de sigilo.
>
> Convém que o treinamento em conscientização comece com um processo formal de indução concebido para introduzir as políticas e expectativas de segurança da informação da organização, antes que seja dado o acesso às informações ou serviços. Convém que os treinamentos em curso incluam requisitos de segurança da informação, responsabilidades legais e controles do negócio, bem como o treinamento do uso correto dos recursos de processamento da informação, como, por exemplo, procedimentos de log-on, o uso de pacotes de software e informações sobre o processo disciplinar.

Portanto, essas constatações reforçam a necessidade da institucionalização da política. E, nesse sentido, entende-se que a unidade com competência por tal elaboração é a Secretaria-Geral, uma vez que o PSI define que "as decisões acerca de Segurança Institucional caberão ao gestor de segurança institucional, que será o titular da Secretaria-Geral".

Recomendação: Recomenda-se à Secretaria-Geral que institua a Política de Gestão Documental do CNMP, conforme, item 4.1, d.2.1, III, do Plano de Segurança Institucional.

Orientação: Orienta-se à Secretaria-Geral que, após a publicação da Política de Gestão Documental, adote medidas para promover ações de conscientização, educação e treinamento em segurança da informação da documentação do CNMP, conforme art. 18, do PSI.

5. Questão de Auditoria 3 - Segurança da Informação de Áreas e Instalações

A Segurança da Informação nas áreas e instalações refere-se às medidas adotadas para proteger informações sensíveis ou sigilosas armazenadas ou em trâmite no espaço físico sob a responsabilidade da instituição ou no espaço físico onde estejam sendo realizadas atividades de interesse da instituição

A QA 3 pretendeu analisar a suficiência das medidas adotadas em áreas e instalações para preservar a integridade, sigilo, autenticidade e disponibilidade das informações armazenadas no CNMP. Verificaram-se os seguintes aspectos:

- Procedimentos de monitoramento e controle de acesso nas áreas de armazenamento de documentos e arquivos;

- Condições de infraestrutura e instalações nas áreas de arquivo do CNMP.

As unidades que dispõem de sala de arquivo foram questionadas acerca do controle de acesso exercido sobre esses espaços e das pessoas cujo ingresso está autorizado.

Em resposta à SAUDI nº 26/2020 - SEI 0383834, a Secretaria Processual (SPR) informou (Despacho SPR – SEI 0384097) que os arquivos permanecem fechados e só são abertos para as seguintes finalidades: arquivamento, desarquivamento, limpeza ou dedetização, sempre previamente autorizado pela unidade.

Estão autorizados a ingressar nos arquivos os servidores da SPR ou terceirizados acompanhados. Quando há necessidade do ingresso de pessoas estranhas à Secretaria, como serventes de limpeza, servidores da engenharia, seguranças, dentre outros, são acompanhados por um servidor da Secretaria.

Em atenção à SAUDI nº 25/2020 - SEI 0383831, a Secretaria de Administração (SA) encaminhou o Despacho COOFIN – SEI 0384621 que esclarece que seu arquivo possui três controles de acesso. O primeiro deles é por meio do sistema Fênix, que controla a movimentação dos processos físicos armazenados. O segundo controle refere-se à localização do arquivo, que é distante das áreas de maior circulação de pessoas e dos processos correntes. A sala de arquivo é fechada com chaves, cuja posse fica com a unidade e com a equipe de segurança do CNMP. O terceiro controle refere-se a forma de acondicionamento dos processos na sala de arquivo.

Segundo a unidade, “os processos físicos foram acondicionados, de maneira organizada, em arquivos deslizantes eletrônicos com senha de segurança digital e também chave física”. Por fim, informou que o acesso é restrito aos colaboradores da unidade: servidores, estagiária e prestadora de serviços. Destacou, ainda, que a sala, há um ano, é compartilhada com outra coordenadoria da Secretaria de Administração, a COGCS.

A Corregedoria Nacional, em resposta à SAUDI nº 27/2020 - SEI 0383839, encaminhou o Memorando nº 12/2020/COGE - SEI 0385224, em que esclarece que as chaves dos arquivos da Corregedoria ficam a cargo de uma assessora de gabinete, mas todos os servidores e terceirizados são autorizados a ingressar e anexar documentos e pastas quando necessário.

5.1 Constatação: Inexistência de sistema de alarme ou videomonitoramento no arquivo da SGP

Análise: Quanto ao monitoramento das áreas de armazenamento de documentos e arquivos, a NUSEG/COSET/SA informou no Despacho NUSEG – SEI 0377363 que o CNMP não dispõe de sistema de alarme, contudo, há sistema de videomonitoramento que cobre todas as entradas dos arquivos, com exceção do arquivo da SGP.

Cabe ressaltar que as câmeras de monitoramento foram verificadas em fevereiro de 2020, no âmbito da Auditoria de Segurança Institucional, conforme item 4 do Relatório e papel de trabalho “Inspeção câmeras 18.02”. Sobre este ponto, o Relatório informa que:

> Foi verificada a existência e o posicionamento das câmeras de videomonitoramento, de acordo com o Contrato CNMP nº 47/2016, bem como o funcionamento de todas elas na sala de monitoramento do CFTV. De acordo com esse critério, a vigilância remota do perímetro interno e adjacente ao CNMP é realizada por 76 câmeras e não foram encontradas divergências.

O documento "Recomendações para a construção de arquivos" (CONARQ, 2000), no tocante à proteção contra roubo e vandalismo (item 10.2 do referido texto), sugere que sejam instalados sistemas de alarme ou outros dispositivos.

Recomendação: Recomenda-se à Secretaria de Gestão de Pessoas que avalie o risco de permanecer sem sistema de alarme ou videomonitoramento na sala de arquivo da SGP e, caso entenda necessário, que envide os esforços necessários à contratação desses artefatos.

5.2 Informação: Brigada não capacitada para o resgate de acervos em caso de incêndio

Análise: A publicação “Recomendações para a construção de arquivos” – CONARQ, 2000, no item 10.1 trata da proteção dos arquivos contra fogo e água. Além do cuidado nas instalações elétrica e hidráulica e em suas manutenções, o documento versa sobre a proteção adequada contra o fogo. Informa que extintores devem ser distribuídos pelos depósitos e, se possível, deve-se utilizar extintores automáticos, do tipo aspersores ou sprinklers, mais recomendáveis para depósitos de documentos. Conclui pela necessidade de que a brigada de incêndio da instituição seja treinada para colaborar no salvamento do acervo.

A SAUDI nº 17/2020 - SEI 0376662 questionou a Secretaria de Administração sobre a existência de extintores de incêndio nas salas que abrigam processos ou outros documentos físicos e se são do tipo aspersores. Questionou, ainda, sobre a capacitação da brigada de incêndio para resgate do acervo.

Quanto aos extintores de incêndio, a unidade informou que os utilizados pelo CNMP são do tipo CO^2 e estão localizados no acesso ou próximo ao acesso de todas os arquivos. Atualmente, o Conselho não dispõe de sistema de combate a incêndio por aspersores (sprinkler).

A NUSEG/COSET/SA informou no Despacho NUSEG – SEI 0377363 que a brigada de incêndio não tem capacitação específica para atuar no resgate de acervos. Cabe acrescentar que o Contrato-CNMP nº 28/2016, cujo objeto é a prestação de serviços contínuos de segurança contra incêndio, pânico, abandono de edificação e primeiros socorros por meio de equipe de brigadistas particulares, não exige esse tipo de capacitação, tampouco o termo de referência respectivo.

Em reposta à matriz de achados, a unidade mencionou a Resolução CONARQ nº 34/2012, que trata sobre o resgate de acervos danificados por água ou fogo. A Resolução recomenda que as instituições possuam grupo de trabalho para o momento de crise, com representantes da alta administração, da área administrativa e do

responsável pelo acervo. Esse grupo viabilizaria ações administrativas para auxiliar o trabalho dos técnicos responsáveis pelo resgate do acervo. Nesse contexto, a unidade sugere que:

> a equipe de brigada receba orientações, de pessoas que trabalhem diretamente com os acervos do CNMP, sobre qual o acervo mais importante para a instituição e como poderá colaborar preventivamente e efetivamente em casos de sinistros.

Dessa forma, observa-se que a elaboração e publicação da Política de Gestão Documental do CNMP e a definição da unidade responsável por essa gestão é fundamental para sanar definitivamente o apontamento deste tópico, pois a segurança da informação de áreas e instalações impacta, sobretudo, a disponibilidade das informações.

Ações pontuais que corrijam falhas específicas de infraestrutura e segurança não são suficientes para sanar a deficiência principal na gestão dos arquivos do CNMP: a falta de normatização própria para a gestão documental.

6. Questão de Auditoria 4 - Segurança da Informação de Recursos de TI

Segurança da informação nos recursos de TI é um conjunto de medidas destinadas a salvaguardar dados e informações sensíveis ou sigilosos gerados, armazenados e processados por intermédio da TI, bem como a própria integridade dos sistemas de informação utilizados no CNMP.

Nesse contexto, esta QA teve como finalidade verificar a suficiência das medidas adotadas para preservar a integridade, sigilo, autenticidade e disponibilidade das informações armazenadas no CNMP por intermédio da TI. Para a análise, foram verificados os seguintes itens:

- Regulamentação do macroprocesso Gestão da Segurança da Informação nos ativos de TI;
- Política de Segurança da Informação para os recursos de TI;
- Plano de Continuidade do Negócio de TI;
- Política de Controle de Acesso;
- Política de Senhas;
- Acesso à internet e utilização da rede de dados corporativa; e
- Acesso aos sistemas e arquivos do CNMP por meio do VPN.

Formalmente, o CNMP elaborou a Política de Segurança Institucional e o Plano de Segurança Institucional, Portarias CNMP-PRESI n° 153/2017 e 167/2018, respectivamente, dos quais a segurança da informação é uma parte do conteúdo.

Assim, a segurança da informação está dividida 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° 153/2017.

Nesse contexto, foi analisada a aderência das diversas normas relacionadas à segurança da informação nos ativos de TI no CNMP às boas práticas propostas pelo TCU no item 1.3 do manual “Boas Práticas em Segurança da Informação”, 4ª edição. De maneira geral e abrangente, os normativos vigentes no CNMP abordam parte do conteúdo indicado pela Corte de Contas.

Entretanto, as orientações poderiam ser mais assertivas se houvesse um normativo específico para TI, já que o arcabouço normativo do CNMP é para a segurança institucional como um todo. Observou-se que não há política de continuidade dos serviços de TI, política de controle de acesso ou política de senhas formalizadas.

6.1 Informação: Ausência de regulamentação do macroprocesso Segurança da Informação nos ativos de TI

A regulamentação do macroprocesso Gestão da Segurança da Informação nos ativos de TI está prevista na Resolução CNMP nº 171/2017, que institui a Política Nacional de Tecnologia da Informação do Ministério Público e se aplica ao CNMP.

De acordo com o art. 18 da referida norma, a segurança da informação nos ativos de TI é um dos sete macroprocessos que devem ter a gestão regulamentada para garantir que os ativos críticos, os riscos, as ameaças, as vulnerabilidades e os incidentes de segurança sejam identificados, monitorados e priorizados por meio de controles efetivos:

> Art. 18. As unidades e os ramos do Ministério Público deverão regulamentar a gestão dos seguintes macroprocessos de TI:
>
> I – portfólio, programas e projetos de TI;
>
> II – riscos de TI;
>
> III – serviços de TI;
>
> IV – continuidade dos serviços de TI;
>
> V – sistemas de informação;
>
> VI – infraestrutura de TI;
>
> VII – **segurança da informação nos ativos de TI**. (grifo nosso)

Ainda de acordo com o normativo, o macroprocesso em questão deve contemplar a continuidade dos serviços de TI e o uso dos ativos de TI, conforme art. 28.

Com o objetivo de implementar a Resolução, a STI encaminhou à Secretaria-Geral, por meio do Processo SEI nº 19.00.6300.0005143/2020-41, Minuta de Portaria que institui a Política de Governança e Gestão de Tecnologia da Informação do CNMP (PGGTI-CNMP).

Contudo, de acordo com Despacho SG/SEC - SEI 0379788, os autos retornaram à STI para providências em conjunto com a Assessoria Jurídica (ASJUR). Trata-se da adequação da Minuta de portaria às alterações do Modelo de Governança e Gestão Integrada da Estratégia. (MGGIE).

Destaca-se que essa política formaliza de forma mais detalhada e efetiva as ações que visam preservar a segurança da informação nos ativos de TI.

6.2 Informação: Ausência de Plano de Continuidade dos Serviços de TI

Em reposta à SAUDI nº 20/2020 – SEI 0376700, o Secretário de TI informou, por meio do Despacho STI – SEI 0379379, que não existe o documento citado, porque o CNMP não possui um Plano de Continuidade do Negócio, que é a referência a partir da qual o Plano de Continuidade dos Serviços de TI seria elaborado.

Entretanto, no Plano Diretor de Tecnologia da Informação (PDTI) há a sessão "Contingência Operacional de TI" que inclui algumas das medidas adotadas com a finalidade de reduzir ao mínimo possível o risco de indisponibilidade dos serviços de TI do CNMP:

> Despacho STI 0379379
>
> Plano de Continuidade dos Serviços de TI e está diretamente vinculado ao Plano de Continuidade do Negócio, uma vez que os serviços de TI se propõem a automatizar e a entregar valor aos processos da cadeia de valor.
>
> Não existindo o Plano de Continuidade do Negócio é inviável que exista o Plano de Continuidade dos Serviços de TI. No entanto, sabendo-se da importância de prever medidas de contingência e garantia de funcionamento dos serviços oferecidos, a Secretaria incluiu em seu Plano Diretor de TI uma sessão onde descreve as contingências operacionais de TI.
>
> Essas contingências baseiam-se primordialmente na salvaguarda de ativos que suportam cada um dos serviços e sistemas de Tecnologia da Informação no CNMP e incluem a realização de testes periódicos nas situações em que isso seja necessário.

De acordo com o as boas práticas indicadas pelo TCU, é importante que exista o Plano de Continuidade dos Serviços de TI, pois, atualmente, o funcionamento das instituições de modo geral depende vitalmente das informações armazenadas e processadas pela TI.

Além disso, a Corte de Contas aborda, no item 3.6 do Manual "Boas Práticas em Segurança da Informação", a necessidade de comprometimento da Alta Administração para a elaboração do referido documento. De acordo com o Manual:

> Na verdade, este Plano é de responsabilidade direta da alta administração, é um problema corporativo, pois trata de estabelecimento de procedimentos que garantirão a sobrevivência da instituição como um todo e não apenas da área de informática. Ainda, muitas das definições a serem especificadas são definições relativas ao negócio da instituição e não à tecnologia da informação.

Desse modo, alerta-se quanto à necessidade da elaboração do referido documento pela STI, com o apoio da Alta Administração.

Em que pese a ausência desse Plano, destaca-se que durante o período de trabalho remoto, que perdura desde meados de março até o presente momento, não houve interrupção dos sistemas e serviços oferecidos pela TI do CNMP, o que demonstra a boa gestão desses serviços.

Na atual conjuntura, que é considerada uma contingência, foi possível dar continuidade aos serviços do CNMP com a utilização da Virtual Private Network (Rede Privada Virtual) ou VPN1.

Questionou-se na SAUDI n° 22/2020 - SEI 0377048 sobre a confidencialidade, integridade, disponibilidade e autenticidade das informações nos acessos aos sistemas e arquivos do CNMP por meio da VPN. Em resposta, por meio do Despacho STI – SEI 0379969, a Secretaria informou:

> A confidencialidade é garantida pelo túnel criptografado que é configurado após o usuário estabelecer a conexão VPN. Após o estabelecimento desta conexão, todas as informações enviadas e recebidas serão criptografadas.
>
> A utilização de dispositivos redundantes, tais como links de internet, balanceadores de carga, firewall e servidores de aplicação garantem a disponibilidade dos recursos. Além dos clusters de alta disponibilidade, softwares de monitoramento verificam os equipamentos e emitem alertas ao detectarem sobrecarga ou falhas.
>
> A VPN, por si só, não tem o propósito de garantir a integridade e autenticidade das informações. Estas características são garantidas por outros softwares/aplicativos que podem ou não utilizar o túnel VPN para trafegar os dados.

Assim, observou-se que a TI do CNMP demonstrou capacidade de aplicar os procedimentos necessários para manter o funcionamento da instituição sem comprometer a segurança das informações do órgão. Contudo, a boa execução desses procedimentos não diminui a importância da elaboração do Plano de Continuidade dos Serviços de TI, pois o plano tem por finalidade institucionalizar os procedimentos mencionados.

Orientação: Orienta-se à Secretaria de Tecnologia da Informação que, com a elaboração do Plano de Continuidade de Negócios do CNMP, envide esforços para elaborar e publicar o Plano de Continuidade dos Serviços de TI.

6.3 Constatação: Ausência de aferição dos indicadores do PDTI relativos à Segurança da Informação

Análise: Verificou-se que no Plano Diretor de Tecnologia da Informação (PDTI 2019/2021) existe um objetivo de contribuição relacionado à segurança da informação: "Aprimorar a segurança da informação nos ativos de TI - Aprimoramento contínuo de políticas e ferramentas para que sejam mantidos os controles de segurança da informação adequados nos ativos de TI".

Relacionados a esse objetivo, existem 3 indicadores:

Índice de atualização de softwares de sistema: Mensura a atualização dos softwares de sistema que dão sustentação aos demais softwares utilizados.	Periodicidade da coleta: trimestral
	Frequência da meta: anual, sendo 50% em 2019 e 70% em 2020
Índice de conformidade das estações de trabalho: monitora as atualizações de versões do conjunto mínimo de softwares instalados nos microcomputadores do parque tecnológico do CNMP	Periodicidade da coleta: trimestral
	Frequência da meta: anual, sendo 75% em 2019 e 85% em 2020
Índice de testes de recuperação bem-sucedidos: Avalia a eficiência da recuperação das cópias de segurança dos dados corporativos	Periodicidade da coleta: mensal
	Frequência da meta: anual, sendo 4 em 2019 e 12 em 2020

De acordo com o PDTI, item 1.2, o acompanhamento de sua execução ocorrerá quadrimestralmente nas Reuniões de Acompanhamento Tático (RAT), ocasiões em que "será avaliado o cumprimento das ações e indicadores previstos(...)".

Todavia, não se identificou a aferição de desempenho dos referidos indicadores. Foram analisadas as atas da 21ª e 22ª RAT, as atas da 11ª, 12ª e 13ª reuniões do SETI, além da 14ª reunião do SERSI, todas realizadas em 2019, e não houve registro sobre o assunto. Em 2020, em razão da suspensão das atividades presenciais no CNMP, não se realizou a RAT do primeiro quadrimestre, sendo previstas apenas 2 reuniões de acompanhamento tático: 26/08/2020 e 02/12/2020.

Como boa prática, o Tribunal de Contas da União recomenda, no manual "Boas Práticas em Segurança da Informação" que sejam feitas, periodicamente, análises sobre a efetividade da segurança da informação nas instituições. Assim, a ausência da medição desses indicadores prejudica o monitoramento da efetividade da segurança da informação nos ativos de TI e não se coaduna com as boas práticas recomendas pelo TCU.

Em resposta à Matriz de Achados encaminhada pela SAUDI nº 35/2020 - SEI 0389306, a STI informou que a coleta dos indicadores ficou integralmente prejudicada em função da necessidade de rápida adaptação ao regime de trabalho remoto, em função da pandemia mundial de COVID-19, de acordo com o Despacho STI-SEI 0393888. Assim, a Secretaria se voltou para as atividades operacionais, em detrimento do acompanhamento dos indicadores. Pelo mesmo motivo, não foram realizadas reuniões do SETI no período.

É compreensível que os esforços empregados pela STI para assegurar o funcionamento de todos os sistemas do CNMP, de modo a sustentar as atividades do Órgão, tenham impedido a coleta dos dados e a aferição dos indicadores a partir de março de 2020. Contudo, o PDTI, aprovado em outubro de 2019, já previa meta para aquele ano, e não há informações sobre o respectivo monitoramento.

Assim, com a finalidade de "Aprimorar a segurança da informação nos ativos de TI", é recomendável que, tão logo seja possível, a unidade envide esforços no sentido de realizar o necessário monitoramento dos indicadores do seu Plano Diretor.

Recomendação: Recomenda-se à Secretaria de Tecnologia da Informação que realize o adequado acompanhamento dos indicadores previstos no PDTI, em cumprimento ao previsto no item 1.2 do referido documento.

6.4 Constatação: Ausência de normatização sobre regras de inspeção automatizada de tráfego.

Análise: De acordo com o item 4.1, d.4, tópico "Do acesso à internet", do Plano de Segurança Institucional:

> 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;

Em consulta às normas vigentes no âmbito do CNMP, em especial no que se refere à Segurança da Informação, não se identificou regulamento que estabeleça regras de inspeção automatizada de tráfego visando a mitigar incidentes de segurança e a otimizar a utilização dos canais de acesso à internet, contrariando o descrito no Plano de Segurança Institucional do CNMP.

Em resposta a Matriz de Achados (SAUDI nº 35/2020 - SEI 0389306), a STI afirmou que "embora não haja normativo para isso, atualmente é feita inspeção automatizada de tráfego visando a mitigar incidentes de segurança e a otimizar a utilização dos canais de acesso à internet".

Recomendação: Recomenda-se à Secretaria de Tecnologia da Informação que elabore instrumento normativo complementar estabelecendo regras de inspeção automatizada de tráfego visando a mitigar incidentes de segurança e a otimizar a utilização dos canais de acesso à internet, conforme previsto no tópico 4.1, d.4 do Plano de Segurança Institucional.

6.5 Constatação: Usuários sem exercício atual no CNMP com acesso ativo ao *Microsoft Office365*

Análise: Em resposta à SAUDI nº 22/2020 - SEI 0377048, a STI encaminhou a lista de contas ativas do *Office 365*, incluindo usuários e unidades do CNMP no dia 13/07/2020 - SEI 0380337. Em alguns casos, as informações vinculadas ao usuário da conta estão diferentes do que consta nos assentos funcionais registrados no sistema MentoRH. Ademais, identificaram-se usuários cedidos com contas habilitadas.

Em resposta à SAUDI nº 29/2020 - SEI 0386935, o Despacho NGS 0387838 informa que não existe verificação periódica da lista de usuários dos sistemas, sendo realizada apenas sob demanda.

De acordo com o estabelecido no Plano de Segurança Institucional - Do Cadastro e Manutenção das Credenciais de Usuários, item V, a STI deve receber a informação acerca das alterações de pessoal para que possa regularizar os respectivos acessos aos recursos de TI:

> 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;

Ainda, em resposta à Matriz de Achados – SEI 0393888, a STI informou:

> Sobre a atualização dos dados (nome e setor) da base do Office 365 em consonância com os dados do Mentorh, esta STI entende que essa validação deveria ser iniciada pela SGP, dado que a área é a gestora negocial das informações de pessoal.
>
> (...)
>
> Por fim, sobre os usuários cedidos ainda habilitados, cabe à SGP definir a regra para remoção ou não dessas contas, dado que a STI não tem competência para definir tal questão e os usuários ainda precisam interagir com alguns recursos, como email, segundo a própria Secretaria de Gestão de Pessoas. Para este ponto, existe processo instruído pela STI com proposta de encaminhamento (19.00.6320.0004564/2020-48), aguardando manifestação da SGP.

Essa lacuna no fluxo de informações já foi tratada no item 3.6 do Relatório de Auditoria nº 3/2019:

> Frise-se que, de acordo com a listagem de usuários ativos, o quantitativo de licenças E3 já alcançou o máximo contratado, enquanto o quantitativo de licenças E1 está bem próximo de alcançar esse quantitativo (350 licenças para cada tipo).
> Dessa forma, faz-se necessária uma gestão contratual adequada, assim como um fluxo de informação eficiente, no sentido de atualizar as licenças dos usuários a fim de possibilitar a inclusão de novos usuários à medida da demanda do órgão.

Com o objetivo de solucionar o gerenciamento dos acessos aos arquivos e sistemas existentes no CNMP, a STI iniciou o desenvolvimento do Sistema de Gestão de Colaboradores, que permitirá, entre outros, o gerenciamento automático de perfis dos sistemas do CNMP e o gerenciamento das assinaturas *Microsoft Office 365* utilizadas pelos colaboradores do CNMP, conforme Processo nº 19.00.6320.0004564/2020-48.

Ressalta-se a necessidade de observância ao princípio da economicidade. De acordo com a Nota Técnica 01 - SEI 0372479, constante do referido processo:

> Ainda que a licença E1 seja menos onerosa que uma licença E3, ela ainda custa R$ 331,49 ao ano para o CNMP (vide Ata de Registro de Preço CPL 0343873). Complementarmente, informamos que a licença E3 custa ao ano para o CNMP o valor de R$ 968,12.

Ante o exposto, os autos foram encaminhados à SGP para manifestação sobre as especificidades da gestão de pessoas do Órgão, conforme Despacho STI – SEI 0372871. Não obstante, na reunião de encerramento da auditoria, o Secretário de TI informou que o Sistema já está em fase de testes, o que foi demonstrado à COAUD no dia 11/09/2020, por meio do Teams.

Assim, finalizados os testes do Sistema ele já entrará em operação, e, quando definido pela Administração o tratamento direcionado aos servidores sem efetivo exercício no CNMP, mas não desligados, os parâmetros serão incorporados ao Sistema para gerenciamento automático das contas do *Microsoft Office365*.

Recomendação: Recomenda-se à Secretaria de Gestão de Pessoas que defina os parâmetros para gerenciamento das assinaturas *Microsoft Office365* dos servidores sem efetivo exercício no CNMP.

VI – MONITORAMENTO

1. Relatório de Auditoria nº 03/2019

Recomendação 5.1: Recomenda-se à Secretaria Processual que regularize os perfis e níveis de acesso dos usuários do Sistema ELO, concedendo a cada usuário previsto na Portaria CNMP-PRESI n° 63/2015.

Análise: Em análise à planilha de usuários do sistema ELO no dia 30/06/2020 (SEI 0384821), juntada aos autos em resposta à SAUDI 28/2020 - SEI 0384290, não foram encontrados usuários com nível de acesso maior que o permitido pela Portaria CNMP-PRESI n° 63/2015. Contudo foram identificados perfis ativos que, aparentemente, deveriam estar desativados:

- RAQUEL ELIAS FERREIRA DODGE - Nível 5 (Fim de mandato);
- ROSE MEIRE CYRILLO - Nível 4 (Fim de designação); e
- BRUNA LARISSA DE BRITO MONTEIRO - Nível 3 e 5 (movimentação interna).

Em resposta à Matriz de Achados, a Secretaria informou, por meio do Despacho SPR – SEI 0391061, que não recebeu o nada consta dessas pessoas e que já realizou a exclusão desses perfis do Sistema ELO.

Observa-se que há uma falha no fluxo de comunicação entre a unidade de gestão de pessoas e as unidades responsáveis pelos sistemas do CNMP. O Processo SEI 19.00.6320.0004564/2020-48 trata do desenvolvimento de sistema que permitirá o gerenciamento automático de perfis de acesso aos sistemas do CNMP, conforme análise do item 6.5 deste relatório.

Dessa forma, considera-se a recomendação 5.1 do Relatório de Auditoria nº 03/2019 **implementada**.

VII. CONCLUSÃO

Ante o exposto, é possível afirmar que as medidas adotadas até o momento foram suficientes para preservar a segurança da informação de pessoas e, assim, proteger informações sensíveis ou sigilosas.

Além disso, o CNMP dispõe de medidas adequadas e razoáveis para garantir a segurança da informação na documentação. Contudo, no que se refere à gestão documental, o CNMP ainda carece da elaboração da Política de Gestão Documental e da definição da unidade responsável pelo tema.

Em consequência da falta dessa Política, foram encontradas deficiências nas instalações físicas destinadas a guarda de documentos do CNMP.

Quanto à segurança da informação nos ativos de TI, até o momento as ações adotadas foram suficientes para preservar a integridade, sigilo, autenticidade e disponibilidade das informações armazenadas no CNMP por intermédio da TI. Contudo, a falta de normatização de mecanismos de governança e gestão específicos de TI trazem o risco da não institucionalização dos procedimentos, o que torna a boa gestão desses serviços muito dependente das pessoas, em vez de aprimorar os processos da instituição.

Nestes termos, encaminha-se à Presidência para ciência e à Secretaria-Geral para adoção de providências quanto aos itens 4.4 e 4.5, à Secretaria de Tecnologia da Informação para adoção de providências quanto aos itens 6.3 e 6.4, à Secretaria Processual para adoção de providências quanto ao item 4.2, à Secretaria de Gestão de Pessoas para adoção de providências quanto aos itens 5.1 e 6.5a, e à Ouvidoria para adoção de providências quantos ao item 4.3a e 4.3b.

Brasília, 14 de setembro de 2020.

DANIELA CARVALHO RAMOS GHERSEL
Analista de Gestão Pública

JOSIAS MENDES DA SILVA
Analista de Gestão Pública

À consideração do Auditor-Chefe.

BÁRBARA GOMES ARAUJO FERNANDES
Coordenadora de Auditoria Substituta

De acordo, encaminhe-se na forma proposta.

ANTONIO GOMES FERREIRA
Auditor-Chefe

APÊNDICE I – RECOMENDAÇÕES DO RELATÓRIO DE AUDITORIA Nº 3/2020

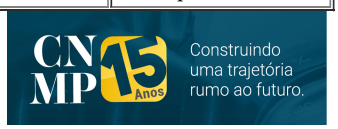
Quadro Consolidado das Recomendações da Auditoria Interna

Item	Recomendação	Unidade
4.2	Recomenda-se à Secretaria Processual que promova a adequação das regras de aposição de sigilo no sistema SEI ou da legislação vigente.	SPR
4.3 a	Recomenda-se à Ouvidoria Nacional que os extratos das informações sobre classificação e desclassificação de sigilo publicados no Portal da Transparência do CNMP contemplem todos os requisitos exigidos pelo item 4.1, d.2.1, XI, do Plano de Segurança Institucional.	OUV
4.3 b	Recomenda-se à Ouvidoria Nacional que avalie quanto à inclusão, no rol das informações sigilosas divulgadas no Portal da Transparência, dos processos com classificação de sigilo no SEI, em atendimento ao item 4.1, d.2.1, XI, do Plano de Segurança Institucional.	OUV
4.4	Recomenda-se à Secretaria-Geral que envide esforços no sentido de promover a publicação do Plano/Código de Classificação e a Tabela de Temporalidade e Destinação de Documentos do CNMP, abrangendo tanto a área-meio quanto à área fim da Instituição.	SG
4.5	Recomenda-se à Secretaria-Geral que institua a Política de Gestão Documental do CNMP, conforme, item 4.1, d.2.1, III, do Plano de Segurança Institucional.	SG
5.1	Recomenda-se à Secretaria de Gestão de Pessoas que avalie o risco de permanecer sem sistema de alarme ou videomonitoramento na sala de arquivo da SGP e, caso entenda necessário, que envide os esforços necessários à contratação desses artefatos.	SGP
6.3	Recomenda-se à Secretaria de Tecnologia da Informação que realize o adequado acompanhamento dos indicadores previstos no PDTI, em cumprimento ao previsto no item 1.2 do referido documento.	STI
6.4	Recomenda-se à Secretaria de Tecnologia da Informação que elabore instrumento normativo complementar estabelecendo regras de inspeção automatizada de tráfego visando a mitigar incidentes de segurança e a otimizar a utilização dos canais de acesso à internet, conforme previsto no tópico 4.1, d.4 do Plano de Segurança Institucional.	STI
6.5	Recomenda-se à Secretaria de Gestão de Pessoas que defina os parâmetros para gerenciamento das assinaturas *Microsoft Office365* dos servidores sem efetivo exercício no CNMP.	SGP

APÊNDICE II – MONITORAMENTO DE RECOMENDAÇÕES ANTERIORES

Quadro Consolidado das Recomendações da Auditoria Interna
Relatório nº 3/2019

Item	Recomendação	Status
5.1	---	Implementada



Documento assinado eletronicamente por **Antonio Gomes Ferreira**, **Auditor Chefe do CNMP**, em 14/09/2020, às 18:04, conforme Portaria CNMP-PRESI Nº 77, DE 8 DE AGOSTO DE 2017.

Documento assinado eletronicamente por **Barbara Gomes Araujo Fernandes**, **Coordenador(a) de Auditoria substituto(a)**, em 14/09/2020, às 18:08, conforme Portaria CNMP-PRESI Nº 77, DE 8 DE AGOSTO DE 2017.

Documento assinado eletronicamente por **Daniela Carvalho Ramos Ghersel**, **Analista de Gestão Pública**, em 14/09/2020, às 19:19, conforme Portaria CNMP-PRESI Nº 77, DE 8 DE AGOSTO DE 2017.

A autenticidade do documento pode ser conferida no site https://sei.cnmp.mp.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0399289** e o código CRC **56667684**.