DISPONIBILIDADE DE SERVIÇOS DE TI

Auditoria de Avaliação Operacional (AO) n° 12 - Paint 2023

Audin/Geauc
2023

Companhia Nacional de Abastecimento – Conab

Presidente da República

Luiz Inácio Lula da Silva

Ministro do Desenvolvimento Agrário e Agricultura Familiar

Luiz Paulo Teixeira Ferreira

Diretor-Presidente da Companhia Nacional de Abastecimento

João Edegar Pretto

Diretor-Executivo de Gestão de Pessoas (Digep)

Lenildo Dias de Morais

Diretor-Executivo Administrativo, Financeiro e de Fiscalização (Diafi)

Rosa Neide Sandes de Almeida

Diretor-Executivo de Operações e Abastecimento (Dirab)

Thiago José dos Santos

Diretor-Executivo de Política Agrícola e Informações (Dipai)

Silvio Isoppo Porto

Chefe da Auditoria Interna

Paulo Ricardo Grazziotin Gomes

Gerente de Auditoria Consultiva (Geauc)

Marcos Paulo Silvério de Oliveira

Equipe de Auditoria

Gidalia Brito

Lista de Quadros

Sumario

1. Introdução

Trata o presente relatório da apresentação dos resultados da Auditoria Operacional (AO) n.º 12, realizada em consonância com o Plano Anual de Atividades da Auditoria Interna – Paint/2023 e tendo como objeto auditável: gestão da disponibilidade de TI.

O objetivo do objeto auditado é:

> *Executar os procedimentos necessários para garantir a disponibilidade dos serviços de TI nos níveis acordados, envolvendo a administração e o monitoramento do ambiente e infraestrutura e a implementação de melhorias.*

Para o tratamento do processo auditado, utilizou-se como suporte e referência de boas práticas o *framework* ITIL, acrônimo para *Information Technology Infrastructure Library* (ou Biblioteca de Infraestrutura de Tecnologia da Informação, em português). A ITIL serve para organizar processos de TI e orientar profissionais no planejamento e execução destes.

A versão 4 da ITIL preconiza 34 processos (práticas). Para esta versão, o propósito da prática "gerenciamento da disponibilidade" é "garantir que os serviços entreguem níveis acordados de disponibilidade para atender às necessidades de clientes e usuários. "

Na prática, a garantia da disponibilidade dos serviços de TI não pode ser obtida por meio de um processo único, mas como a resultante do desenho e implementação de outros processos que envolvem a prestação dos serviços de TI, que precisam estar funcionando de forma eficiente e integrada.

Dessa forma, cabe ao responsável pela prestação desses serviços, por exemplo, criar, manter e gerir uma infraestrutura de TI capaz de dar suporte à execução dos serviços (Gerenciamento de capacidade e desempenho[1], gerenciamento de Ativos de TI[2]), garantir a entrega dos serviços de forma segura (gerenciamento da segurança da informação[3]), manter os serviços

---

1 O propósito da prática de gerenciamento de capacidade e desempenho é garantir que os serviços atinjam o desempenho acordado e esperado, satisfazendo a demanda atual e futura de maneira econômica.

2 O propósito da prática de gerenciamento de ativo de TI é planejar e gerenciar todo o ciclo de vida de todos os ativos de TI (informação, ativos físicos, softwares...), para ajudar a organização na criação ou preservação de valor organizacional.

3 O propósito da prática de gerenciamento da segurança da informação é proteger as informações necessárias organização para conduzir seus negócios. Isso inclui compreender e gerenciar os riscos para a confidencialidade, integridade e disponibilidade de informações – naquilo que se convencionou denominar de tríade CID – bem como outros aspectos da segurança da informação, como autenticação (garantir que alguém é quem afirma ser), não repúdio (garantir que alguém não possa negar que realizou uma ação), legalidade (garantir o cumprimento

funcionando de forma adequada e fazer as correções, em tempo hábil, de eventuais intercorrências que interrompam a prestação dos serviços (gerenciamento de incidentes[4], gerenciamento de problemas[5], controle da mudança[6], dentre outros).

Nesse sentido, além do processo de Gestão da Disponibilidade de TI, avaliou-se como conveniente e oportuno tratar, também, do processo de Gerenciamento da Continuidade, que trata da disponibilidade dos serviços de TI em casos de ocorrência de eventos fortuitos (desastres), e que pode ser visto como um caso particular do processo da disponibilidade:

> *O propósito da prática de gerenciamento de continuidade de serviço é garantir que a disponibilidade e o desempenho de um serviço sejam mantidos em níveis suficientes no caso de um desastre. A prática fornece uma estrutura para a criação de resiliência organizacional com a capacidade de produzir uma resposta eficaz que proteja os interesses dos principais interessados e a reputação, a marca e a criação de valor da organização.*

Para esta auditoria, o conceito de desastre a ser adotado será aquele definido no Plano de Continuidade de Negócios da Conab (PCN) da Conab, apresentado a seguir:

> *Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização, e gera sérios impactos na sua capacidade de entregar serviços essenciais ou críticos, por um período superior ao tempo objetivo de recuperação.*

Este entendimento em relação questão da disponibilidade dos serviços de TI vai ao encontro da visão da Sutin:

> *Não existe um processo de disponibilidade formalmente definido. Atualmente, a SUTIN por meio das suas gerências mantém, como parte de seus esforços de garantia de disponibilidade, estratégias e ferramentas que visam garantir a disponibilidade e desempenho dos serviços de TI sob sua responsabilidade. Como exemplo disto, cita: o monitoramento da infraestrutura, rede de longa distância (SD-WAN) e conexão de Internet redundantes, manutenção da sala-cofre, rotinas de backup corporativo,*

---

da legislação), privacidade (direito da personalidade do indivíduo e que deve permear as relações interpessoais conectadas) e auditoria (capacidade de que seja realizada uma perícia sobre os acessos realizados).

4 O propósito da prática de gerenciamento de incidente é minimizar o impacto negativo dos incidentes restaurando a operação normal do serviço o mais rápido possível.

5 O propósito da prática de gerenciamento de problema é reduzir a probabilidade e o impacto de incidentes, identificando causas reais e potenciais de incidentes e gerenciando soluções alternativas e erros conhecidos.

6 O propósito da prática de controle de mudança é maximizar o número de serviços e produtos de sucesso mudanças, garantindo que os riscos tenham sido devidamente avaliados, autorizando mudanças para prosseguir e gerenciando o cronograma de mudança.

gerenciamento e correlação de eventos de segurança e Antivírus corporativo com prevenção de perda de dados.

Isso posto, para esta auditoria, o conceito do processo de disponibilidade a ser adotado será o do conjunto de processos, subprocessos, procedimentos e ações que são executadas para garantir a disponibilidade dos serviços de TI para os usuários da Conab.

Desta forma, o objetivo do processo auditado citado foi desmembrado em 4 objetivos específicos:

Objetivo 1 – Realizar ações para garantir o fornecimento de ferramentas, *softwares* e infraestrutura requeridos pelo processo, de acordo com os instrumentos de planejamento (PDTIC), de modo a possibilitar o fornecimento dos serviços de TI;

Objetivo 2 – Definir, documentar, instituir e normatizar os processos envolvendo a disponibilidade dos serviços de TI;

Objetivo 3 – Acompanhar e monitorar o fornecimento dos serviços de TI para que estes ocorram em níveis adequados e acordados, executando os ajustes que se fizerem necessários; e

Objetivo 4 – Realizar ações para garantir a continuidade do fornecimento dos serviços de TI em caso de desastres ou falhas[7].

7 Relativamente às atividades de controle, de que trata o item 82 do anexo à IN SFC/CGU nº 3, de 09/06/2017, quando a tecnologia está inserida nos processos de negócios da organização, atividades de controle são necessárias para mitigar o risco de que ela deixe de operar adequadamente no apoio à realização dos objetivos da Companhia (cfe. Estrutura COSO IC-IF 2013, p. 100).

1. Seleção dos Riscos Analisados

Para o desenvolvimento desta auditoria foi utilizada a abordagem de Auditoria Baseada em Riscos (ABR), sendo necessário identificar os riscos envolvidos com o processo de gestão da disponibilidade de TI e, de forma conexa, com o processo de gestão da continuidade da TI.

Para tanto, foram utilizados os riscos pré-identificados no Paint, obtidos a partir de relatórios do sistema Ágatha, gerenciado pela Sucor (instância de 2ª linha), e os riscos identificados durante a fase de entendimento do objeto auditado.

Este estudo resultou na identificação de doze (12) riscos, que foram associados aos quatro objetivos específicos. Em seguida, foi realizada a avaliação do risco inerente, da seguinte forma:

a) para os riscos advindos do sistema Ágatha, a avaliação do impacto e probabilidade foi obtida pela matriz de riscos da Audin; e
b) para os riscos identificados durante o estudo do objeto, a avaliação de impacto e probabilidade foi feita pela equipe de auditoria.

Além disso, foi realizada a avaliação do risco residual, a partir da análise dos controles existentes.

Concluída a avaliação, os riscos foram classificados em termos de magnitude[8] (extremo, alto, médio, baixo e muito baixo), tendo sido selecionados 6 riscos considerados de magnitude extrema ou alta.

Desta forma, os seis riscos selecionados foram:

1) utilização de equipamentos sem garantia, devido à indisponibilidade de recursos financeiros para modernização;
2) investimentos insuficientes em ferramentas e infraestrutura de TI para possibilitar a prestação dos serviços de forma adequada;
3) perda ou Indisponibilidade de *backup* para recuperação de dados;

8 A magnitude é derivada da nota final da avaliação, que é o produto entre a probabilidade e o impacto.

4) baixa maturidade dos processos envolvendo a disponibilidade dos serviços de TI, pois estes não estão formalmente definidos, instituídos, normatizados e documentados;
5) monitoramento não adequado da disponibilidade de sistemas e serviços; e
6) inexistência de um processo definido, implantado e testado para recuperação em caso de desastres.

Cada um destes riscos foi objeto de análise específica, a ser apresentada nos capítulos que se seguem.

2. Análise do Risco 1 — Utilização de equipamentos sem garantia, devido à indisponibilidade de recursos financeiros para modernização

3.1 Apresentação do Risco

A utilização de equipamentos sem garantia pode impactar o processo de Disponibilidade de Serviços de TI, comprometendo o objetivo específico "Realizar ações para garantir o fornecimento de ferramentas, *softwares* e infraestrutura requeridos pelo processo, de acordo com os instrumentos de planejamento (PDTIC), de modo possibilitar o fornecimento dos serviços de TI".

A existência de ativos de TI sem garantia, no parque computacional, pode significar que falhas nestes ativos não tenham solução tempestiva, gerando indisponibilidade dos serviços de TI.

A partir dessa avaliação preliminar, a equipe de auditoria buscou realizar testes de auditoria com o objetivo de responder à seguinte questão:

> "Qual a situação atual dos ativos de TI em uso e sem garantia e quais as medidas tomadas pela Sutin para sanar o problema? "

3.2 Análise do Risco

Para esta análise, utilizou-se de levantamentos dos ativos (*software* e *hardware*) adquiridos e em uso na Conab, com informações acerca da situação desses quanto à garantia. Para aqueles que não possuíam garantia, levantou-se quais as medidas foram adotadas pelo gestor para sanar essa situação. O resultado deste levantamento foi o seguinte:

Quadro 1 – Ativos com garantia

Ano	Nº Contrato	Objeto	Início	Fim	Observações
		Equipamentos de rede			
2013	009	Aquisição de Core de rede central para matriz e superintendências regionais	28/05/2014		
2013	037	Aquisição de comutador de rede central para matriz e superintendências regionais – Termo Aditivo	30/12/2014		Garantia Lifetime
2020	010	Contratação de extensão de garantia e suporte, por 60 (sessenta) meses, para equipamento do tipo Switch Core.	04/03/2020	04/02/2025	Extensão de Garantia do item do

					contrato 009/2013
Equipamento de *Backup*					
2015	020	Aquisição de biblioteca de fitas por meio de adesão à ata de registro de preços nº 66/2013 do Exército Brasileiro - Comando Militar do Sul.	02/10/2015	02/09/2016	
2015	025	Aquisição de módulo para biblioteca de fitas e 20 unidades de fitas LTO-6. Aquisição complementar à OC 20/2015. Adesão à ata de registro de preços Nº 66/2013 do Exército Brasileiro – Comando Militar do Sul.	02/23/2015	02/22/2016	
2018	025	Extensão de Suporte técnico para Oracle StorageTek SL150 e sua respectiva expansão de módulo.	10/18/2018	10/07/2023	Extensão de Garantia do item do contrato 020/2015
Telefonia					
2015	018	Aquisição de solução VOIP, com manutenção, conforme Cláusula Primeira do Contrato e Termo de referência.	12/14/2015	12/11/2016	
2018	010	Fornecimento, mediante registro de preços, de equipamento visando a expansão da solução VoIP existente, para atendimento das necessidades da Conab.	03/26/2018	09/25/2018	
	007	Contratação de serviços de garantia e suporte técnico para a solução de telefonia VoIP da Conab - Avaya Aura, da fabricante Avaya.	03/25/2022	03/25/2023	Extensão de Garantia do item do contrato 018/2015
	007	Extensão da contratação de serviços de garantia e suporte técnico para a solução de telefonia VoIP da Conab - Avaya Aura, da fabricante Avaya.	03/25/2023	03/25/2024	Extensão de Garantia do item do contrato 018/2015
Licenças *Software* infraestrutura					
2015	022	Aquisição de licenças de *software* Microsoft. Windows Server 2012, Windows Server 2012 Dvc Cal, Windows Server 2012 Ext Conn, SQL Server 2014.	12/18/2015	12/17/2016	Suporte até out/2023
Antivírus					
2017	021	Aquisição de novas licenças para atualização da solução de uso perpétuo de antivírus Mcafee, visando a instalação, configuração, garantia, assistência técnica destas novas licenças, e ainda, a renovação e atualização de licenças já existentes, assim como a renovação do Contrato dos serviços de suporte técnico e gerenciamento on site da solução.	07/31/2017	07/30/2018	
2017	021	Suporte do antivírus	07/31/2018	07/30/2019	
2017	021	Suporte do antivírus	07/31/2019	07/30/2020	
2017	021	Suporte do antivírus	07/31/2020	07/30/2021	
2017	021	Suporte do antivírus	07/31/2021	07/30/2022	
	028	Contratação de Solução de Antivírus e Prevenção de perda de dados – DLP da McAfee, com suporte e garantia do fabricante e treinamento técnico especializado.	08/23/2022	08/23/2027	Garantia até 2027
Servidores do datacenter					
2020	011	Aquisição de bens do tipo "Servidor de Rede" conforme especificações, condições, quantidades e exigências detalhadas no	05/22/2020	05/22/2021	Garantia até 2027

		contrato e estabelecidas no termo de referência - anexo I, do edital do pregão eletrônico Conab nº 17/2019.			
2021	001	Aquisição de bens do tipo "Servidor de Rede" conforme especificações, condições, quantidades e exigências detalhadas no contrato e estabelecidas no termo de referência - anexo I, do edital do pregão eletrônico Conab nº 17/2019.	02/12/2021	02/11/2022	Garantia até 2028
Armazenamento no Datacenter					
2021	005	Aquisição de equipamento do tipo Switch Fibre Channel, conforme especificações, condições, quantidades e exigências detalhadas neste Contrato e estabelecidas no Termo de Referência - Anexo I, do Edital de Pregão Eletrônico Conab nº 11/2020.	03/17/2021	09/16/2021	Garantia até 2026
2021	004	Aquisição de solução de armazenamento de dados - Storage, conforme especificações, condições, quantidades e exigências detalhadas neste Contrato e estabelecidas no Termo de Referência - Anexo I, do Edital de Pregão Eletrônico Conab nº 11/2020.	03/03/2021	09/02/2021	Garantia até 2026
Computadores de usuários					
2023	018	Aquisição de estações de trabalho (desktops) e notebooks.	05/23/2023	05/22/2024	Garantia até 2026
2023	019	Aquisição de Worksations.	05/16/2023	06/15/2024	Garantia até 2026

Fonte: Sutin

Quadro 2 – Ativos sem garantia

Ano	Nº Contrato	Objeto	Início	Fim	Impacto	Medidas tomadas pela SUTIN
Equipamentos de rede						
2015	15	Aquisição de 880 impressoras, conforme requisitos técnicos constantes do Termo de Referência.	21/09/2015	20/09/2016	Impressoras possuem mais de 5 anos de uso, todas sem garantia e sem contratos de manutenção, o que pode levar à indisponibilidade dos serviços de impressão. Mesmo com as aquisições de suprimentos sendo realizadas, a falta de garantia implica que esses suprimentos são apenas compatíveis com os originais, porém com qualidade inferior. Esse fator pode acarretar efeitos colaterais na impressão e no próprio funcionamento da impressora. Como resultado, os usuários expressam insatisfação durante a execução de suas atividades, seja devido a interrupções do serviço ou à necessidade de substituição dos suprimentos.	Durante os anos foram adquiridos suprimentos para as impressoras e por meio do processo SEI 21200.003819/2023-47 a GESUT visa a contratação de solução de TI para renovação do parque de impressoras na Matriz e CDRH

2015	25	Fornecimento de 665 Microcomputadores HP Desktop com Windows	29/12/2015	29/12/2020	O serviço de garantia expirou em 13/02/2021. A Matriz e as SUREGs possuem parques computacionais bastante defasados, onde equipamentos com mais de 6 anos de uso e desassistidos pelas garantias de fabricação e manutenção, continuam em funcionamento. Ressalta-se que não há estoque de peças de reposição, ademais, o sistema operacional Microsoft Windows 7 ainda está em uso, expondo o corpo funcional a diversos problemas de ordem da segurança da informação, visto o encerramento de seu suporte técnico em janeiro de 2020 e a inviabilidade de realização de atualizações críticas. Os demais computadores com Windows 8.1 também não possuem mais a garantia de *hardware* e o suporte estendido do sistema operacional findou em janeiro de 2023, parando de receber atualizações críticas e de segurança. Esses equipamentos fora de garantia e/ou obsoletos geram elevados custos de manutenção e demanda por suporte técnico, além de comprometer a produtividade, eficiência e celeridade dos trabalhos da Companhia.	Por meio do processo do processo SEI 21200.002445/2022-61 foi registrada as ARPs 001/2023 e 002/2023 para suprir a necessidade de atualização do parque computacional com meta de 25% (vinte e cinco porcento) ao ano, de acordo com o PDTIC 2021-2024. Até o presente momento foram adquiridos 203 desktops, 47 notebooks e 24 workstations. E foi instruído o processo SEI 21200.003943/2023-11 para renovar mais 25% do parque computacional para o ano de 2024.
2016	19	Aquisição de 341 microcomputadores, conforme especificações constantes da ARP /UFBA.	22/12/2016	21/12/2017	O serviço de garantia expirou em 28/04/2022. A Matriz e as SUREGs possuem parques computacionais bastante defasados, onde equipamentos com mais de 6 anos de uso e desassistidos pelas garantias de fabricação e manutenção, continuam em funcionamento. Esses equipamentos fora de garantia e/ou obsoletos geram elevados custos de manutenção e demanda por suporte técnico, além de comprometer a produtividade, eficiência e	

					celeridade dos trabalhos da Companhia.	
2018	OC 119/2018	Aquisição de 4 iMAC Apple.	18/12/2018	18/12/2020	Garantia de 12 meses, expirada em 18/12/2020, equipamentos adquiridos por meio de DOD, com dispensa de licitação para áreas específicas, que não viram a necessidade de atualizá-los.	
2019	OC 011/2019	Aquisição de 8 notebooks para CONSAD	25/02/2019	25/02/2020	Garantia de 12 meses, expirada em 25/02/2020, equipamentos adquiridos por meio de DOD, com dispensa de licitação para áreas específicas, que não viram a necessidade de atualizá-los.	

Fonte: Sutin

Os ativos com garantia, elencados no Quadro 1, envolvem o núcleo do ambiente operacional de TI, responsável por manter a infraestrutura básica que dá suporte à prestação de Serviços de TI da Companhia, como equipamentos de rede, servidores do datacenter, armazenamento, equipamentos de *backup*, telefonia antivírus etc., o que, sem dúvida, traz uma visão positiva do problema em análise.

Já os equipamentos sem garantia são constituídos basicamente de impressoras (880), microcomputadores (1010) e notebooks (8), conforme se pode verificar no Quadro 2.

3.2.1 Impressoras

Vale ressaltar que o item referente a impressoras tem impacto local na utilização de serviços de TI, isto é, inviabilizando-o apenas para os usuários do serviço em caso de falhas, não tendo impacto sistêmico e, portanto, generalizado em todo ambiente operacional, na disponibilidade dos serviços, tais como servidores de dados e equipamentos do datacenter. Tal fato minimiza, em parte, a gravidade do problema, mas não significa que não deva ser convenientemente tratado.

“Renovar o parque de impressoras da Matriz que se encontram fora de garantia, obsoletas e existe dificuldade na compra de insumos de reposição” é uma das necessidades priorizadas (N13) pelo PDTIC 2021-2024 da Conab, conforme Tabela 4 - Consolidação das Macro Necessidades, deste documento. Em seu item 10. Plano de Metas e Ações, o referido PDTIC detalhou esta necessidade em duas ações, a saber:

AC2 - Elaborar estudo técnico para propor redução de impressoras na Matriz devido à implantação do SEI.

AC3 - Elaborar processo para atualização das impressoras da Matriz nos moldes do RLC.

Em relação às impressoras, a Sutin informa acerca das providências tomadas por meio do processo SEI 21200.003819/2023-47. Neste processo, o ATO DE SUPERINTENDÊNCIA SUTIN N.º 8, DE 26/06/2023, constitui equipe de planejamento objetivando a contratação de solução de TI para renovação do parque de impressoras na Matriz e CDRH, conforme Necessidade N13 e Ações AC2 e AC3 do Plano Diretor de Tecnologia da Informação e Comunicação.

Por tratar-se de ato recente, datado de 26/06/2023, este não surtiu ainda os efeitos desejados. Ressalte-se que a Sutin passou recentemente por uma mudança de gestores, sendo o referido ato já desta nova gestão.

Desta forma, o entendimento desta auditoria é que o problema das impressoras já se encontra devidamente distinguido, documentado e endereçado em termos de providências.

3.2.2 Computadores e Notebooks

Os computadores devem ser vistos de modo distinto àquele das impressoras, em relação ao impacto de ausência de garantia, pois neste caso os efeitos podem ser sistêmicos.

Durante as entrevistas realizadas, a Sutin levantou um ponto que merece atenção.

> *Existem computadores com Microsoft Windows 7 ainda em uso, expondo o corpo funcional a diversos problemas de ordem da segurança da informação, visto o encerramento de seu suporte técnico em janeiro de 2020 e a inviabilidade de realização de atualizações críticas.*

As vulnerabilidades apontadas podem realmente mudar o perfil do impacto, uma vez que, se exploradas e propagadas, podem colocar a segurança em risco, gerando problemas sistêmicos ao ambiente operacional e afetando a prestação de serviços de TI, como um todo.

A propósito destes itens e das providências tomadas, a Sutin faz referência aos processos SEI 21200.002445/2022-61 e 21200.003943/2023-11.

> *Por meio do processo do processo SEI 21200.002445/2022-61 foi registrada as ARPs 001/2023 e 002/2023 para suprir a necessidade de atualização do parque computacional com meta de 25% (vinte e cinco por cento) ao ano, de acordo com o PDTIC 2021-2024. Até o presente momento foram adquiridos 203 desktops, 47 notebooks e 24 workstations.*

O ATO DE SUPERINTENDÊNCIA SUTIN N.º 9, DE 28/06/2023, previsto no processo 21200.003943/2023-11 constitui equipe de planejamento objetivando a contratação de solução de TI para renovação do parque computacional, conforme Necessidade N3 e Ação AC1 do Plano Diretor de Tecnologia da Informação e Comunicação.

De acordo com o PDTIC 2021-2024, a necessidade N3 se refere a "Renovar o parque de computadores e notebooks que se encontram obsoletos e fora de garantia, o que pode causar interrupção nos serviços executados pelas áreas da Companhia" e a ação AC1 consiste de "Elaborar processo de contratação de computadores e notebooks nos moldes do RLC".

Segundo a Sutin, "Esses equipamentos fora de garantia e/ou obsoletos geram elevados custos de manutenção e demanda por suporte técnico, além de comprometer a produtividade, eficiência e celeridade dos trabalhos da Companhia". Inferiu-se que foi possivelmente esta a razão para a escolha da aquisição de novos microcomputadores e notebooks como forma de solucionar o problema da falta de garantia.

Valem aqui as mesmas considerações feitas sobre as impressoras, no sentido de que as providências necessárias foram encaminhadas e que não houve tempo hábil para surtirem efeito e, por fim, que o problema já está adequadamente distinguido, documentado e endereçado.

3.3 Conclusão

Com base nas informações prestadas pela Sutin, os ativos sem garantia se concentram basicamente em impressoras (880) e microcomputadores e notebooks (1018). No que se refere a impressoras, tem-se que o risco de descontinuidade no fornecimento de serviços de TI é local e não sistêmico em caso de falhas agravadas pela falta de garantia.

Já no caso de microcomputadores, a utilização de sistemas operacionais desatualizados por falta de suporte técnico, como o Windows 7, pode significar vulnerabilidades que, se exploradas e propagadas, podem gerar problemas sistêmicos ao ambiente operacional e afetar a disponibilidade dos serviços de TI.

A Sutin demonstrou já ter tomado as providencias adequadas para fazer frente ao problema em ambos os casos, por meio das contratações (aquisições) propostas, que, vale ressaltar, são ações que já se encontravam previstas no PDTIC 2021-2024. Cabe à Companhia envidar

esforços para a disponibilização de recursos para viabilizá-las, haja vista o impacto na disponibilidade dos serviços de TI.

3.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

Estão sendo tomadas ações para renovação do parque computacional. No ano de 2022 foi instruído o processo 21200.002445/2022-61, para atualização de 25% do parque computacional da Companhia, e de onde foram elaboradas as Atas de Registro de Preços 001 e 002/2023, para aquisição de 618 desktops, 84 notebooks e 24 workstations (equipamentos de alto desempenho). Em 2023, através das Atas de Registro de Preços 001 e 002/2023, foram adquiridos 203 desktops, 47 notebooks e as 24 workstations, que foram distribuídos entre a Matriz e as Regionais.

Nessa primeira aquisição, a distribuição de desktops priorizou as regionais com maior índice de equipamentos com o sistema operacional Windows 7. Em 2024, através do processo SEI nº 21200.007917/2023-53, a Ata de Registro de Preços 001/2023 foi totalmente executada, com a assinatura do contrato 003/2024 (SEI nº 33035404) para a aquisição de 415 desktops e 30 notebooks, que serão distribuídos entre Matriz e as Regionais. Está em curso o processo SEI nº 21200.003943/2023-11, que visa a atualização tecnológica de 75% do parque computacional da Companhia, com a aquisição de Desktops (Tipo I, II, III), Notebooks e Workstations de alto desempenho. Também está em curso o processo 21200.001236/2024-62, que visa a contratação de uma empresa especializada no fornecimento do serviço de outsourcing de impressão. Este segundo processo, altera o atual modelo de impressão da Matriz, que abrange várias impressoras distribuídas nos diversos setores. No último levantamento, realizado em 2023, constatou-se a existência de um total de 133 equipamentos de impressão, todos sem garantia e com aquisições eventuais de suprimentos que, devido ao modelo de aquisição, não são originais, são similares.

O novo modelo visa a contratação de empresa especializada para o fornecimento de equipamentos, incluindo software de gerenciamento de ativos e bilhetagem das páginas, assistência técnica de manutenção preventiva e corretiva, treinamento da equipe técnica da

Conab, reposição de peças e insumos/consumíveis (exceto papel). Nesse disponibilizaremos ilhas de impressão, reduzindo o quantitativo de impressoras, que serão distribuídas estrategicamente a modo de atender toda a Matriz.

3. Análise do Risco 2 – Investimentos insuficientes em ferramentas e infraestrutura de TI para possibilitar a prestação dos serviços de forma adequada

4.1 Apresentação do Risco

Investimentos insuficientes em ferramentas e infraestrutura de TI podem impactar o processo de Disponibilidade de Serviços de TI, comprometendo seu objetivo específico "Realizar ações para garantir o fornecimento de ferramentas, *softwares* e infraestrutura requeridos pelo processo, de acordo com os instrumentos de planejamento (PDTIC), de modo possibilitar o fornecimento dos serviços de TI" e causando consequências indesejadas como parque computacional desatualizado e ausência de ferramentas adequadas para a prestação dos serviços de TI, podendo comprometer a disponibilidade desta prestação.

A partir dessa avaliação preliminar, a equipe de auditoria buscou realizar testes de auditoria com o objetivo de responder à seguinte questão:

> "Como tem sido o cumprimento dos investimentos previstos nos dois últimos instrumentos de planejamento (PDTI), para a área de TI? ".

4.2 Análise do Risco

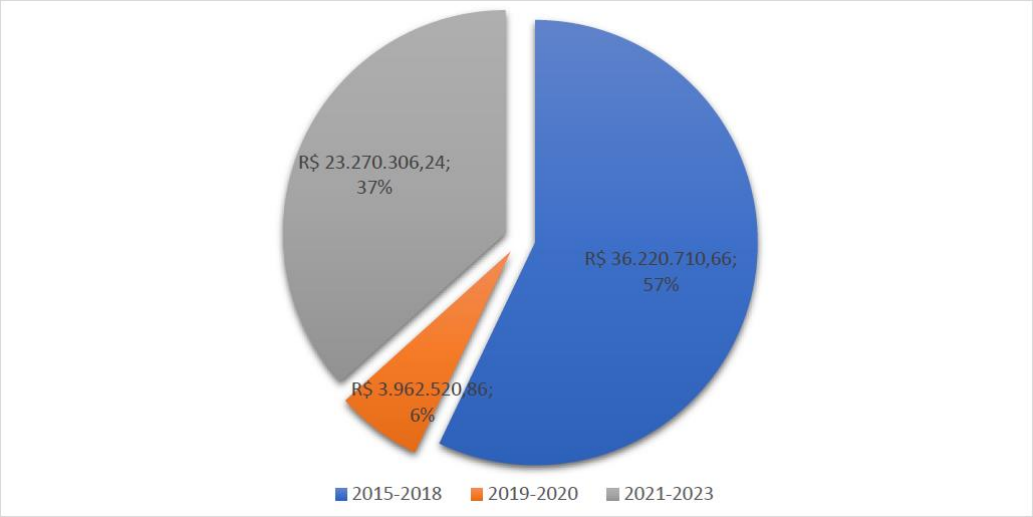
A análise deverá prover subsídios para responder à questão de auditoria citada. Para tanto, foram avaliadas as contratações de bens e serviços de TI efetivamente realizadas entre 2015 e 2023, comparando-as com os investimentos previstos nos instrumentos de planejamento de TI (PDTI 2015-2018 e PDTIC 2021-2024).

4.2.1 Perfil dos investimentos realizados em Tecnologia da Informação, no período de 2015-2023

i. Sob a Perspectiva Temporal

Dentro de uma perspectiva temporal, os investimentos em Reais foram maiores no período 2015-2018 (R$36.220.710,66, correspondendo a 57% do total investido), do que nos anos posteriores, referente ao período 2019-2023 (R$27.232.827,10 correspondendo a 43%). O total investido no período 2015-2023 foi de R$65.453.537,76, a preços correntes.

Gráfico 1 – Investimentos realizados em Tecnologia da Informação (2015-2023)



Fonte: elaborado por Audin.

Cabe lembrar que, para a presente apuração, os dados foram classificados por data de efetivo início da contratação, e não por sua previsão no PDTI a que se refere (pois é possível aditar). Em 2021, por exemplo, durante a vigência do PDTIC 2021-2023, foi executada uma contratação prevista no PDTI 2015-2018).

ii. Maiores Investimentos

As maiores contratações em Tecnologia da Informação ocorreram no período de vigência do PDTI 2015-2018, conforme ranqueamento das maiores aquisições com valor acima de 900 mil reais, exibidas no quadro abaixo.

Quadro 3 – Maiores Aquisições realizadas no período 2015-2024

	Ano	Nº Contrato	Objeto	Início	Fim	Valor Total	Origem
1	2021	013	Contratação de solução de comunicação de dados composta por SD-WAN (*Software* - defined Networking in a Wide Area Network) capaz de prover a interconexão da Matriz da Conab, suas superintendências regionais, suas unidades armazenadoras e as bolsas de mercadoria, entre si e com a Internet, em âmbito nacional, e acesso redundante à Internet, na Matriz.	06/08/2021	06/07/2026	R$ 13.178.230,20	PDTIC 2021-2024

2	2016	012	Contratação para solução de serviços de telecomunicações, por rede IP (Internet Protocol) multisserviços, com tecnologia MPLS, para prover tráfego de voz, dados e imagem, no âmbito de toda Companhia.	06/01/2016	12/01/2018	R$ 10.231.308,00	PDTIC 2015-2018
3	2016	012	TA1	12/01/2018	05/31/2021	R$ 10.231.308,00	PDTIC 2015-2018
4	2016	012	Prorrogação Excepcional	06/01/2021	05/31/2022	R$ 3.191.697,24	PDTIC 2015-2018
5	2015	025	Fornecimento de 665 Microcomputadores HP Desktop com Windows	12/29/2015	12/29/2020	R$ 2.659.933,50	PDTIC 2015-2018
6	2016	007	Contrato emergencial Rede de longa distância (WAN) com a Claro S/A.	06/11/2016	12/08/2016	R$ 2.394.476,16	PDTIC 2015-2018
7	2015	018	Aquisição de solução VOIP, com manutenção, conforme Cláusula Primeira do Contrato e Termo de referência.	12/14/2015	12/11/2016	R$ 1.707.531,76	PDTIC 2015-2018
8	2018	010	Fornecimento, mediante registro de preços, de equipamento visando a expansão da solução VoIP existente, para atendimento das necessidades da Conab.	03/26/2018	09/25/2018	R$ 1.661.021,64	PDTIC 2015-2018
9	2015	015	Aquisição de 880 impressoras, conforme requisitos técnicos constantes do Termo de Referência.	09/21/2015	09/20/2016	R$ 1.471.202,00	PDTIC 2015-2018
10	2016	019	Aquisição de 341 microcomputadores, conforme especificações constantes da ARP /UFBA.	12/22/2016	12/21/2017	R$ 1.431.859,00	PDTIC 2015-2018
11	2022	028	Contratação de Solução de Antivírus e Prevenção de perda de dados – DLP da McAfee, com suporte e garantia do fabricante e treinamento técnico especializado.	08/23/2022	08/23/2027	R$ 1.349.709,60	PDTIC 2021-2024
12	2023	018	Aquisição de estações de trabalho (desktops) e notebooks.	05/23/2023	05/22/2024	R$ 1.199.940,00	PDTIC 2021-2024

13	2020	011	Aquisição de bens do tipo "Servidor de Rede" conforme especificações, condições, quantidades e exigências detalhadas no contrato e estabelecidas no termo de referência - anexo I, do edital do pregão eletrônico Conab nº 17/2019.	05/22/2020	05/22/2021	R$ 944.592,00	PDTIC 2015-2018

Fonte: Audin a partir dos dados da Sutin

iii. Alocação dos investimentos realizados

Quanto ao perfil das contratações, de acordo com os dados apurados no Quadro 4, verifica-se a predominância das contratações voltada para o investimento, em relação àquelas voltadas para o custeio das atividades desenvolvidas.

Quadro 4 – Investimentos por Instância e Natureza – Período 2015-2023

Instância de aprovação	Natureza	Valor	%
PDTIC 2015-2018	Custeio	R$ 5.621.485,80	13,17%
	Investimento	R$ 37.056.001,94	86,83%
	Total	**R$ 42.677.487,74**	100,00%
PDTIC 2021-2024	Custeio	R$ 3.164.105,84	16,32%
	Investimento	R$ 16.228.893,94	83,68%
	Total	**R$ 19.392.999,78**	100,00%
CETI	Custeio	R$ 573.009,32	43,62%
	Investimento	R$ 740.604,24	56,38%
	Total	**R$ 1.313.613,56**	100,00%
Outros	Custeio	R$ 20.325,00	29,27%
	Investimento	R$ 49.111,68	70,73%
	Total	**R$ 69.436,68**	100,00%
Total Custeio		**R$ 9.378.925,96**	14,78%
Total Investimento		**R$ 54.074.611,80**	85,22%
Total Geral		**R$ 63.453.537,76**	100,00%

Fonte: Audin a partir dos dados da Sutin

As aquisições voltadas para o custeio envolvem a contratação de manutenção ou suporte de equipamentos ou serviços já contratados, como manutenção da sala cofre, onde fica o centro de dados, contratação de suporte de *softwares*, aquisição de suprimentos, etc., enfim, envolvem a manutenção do ambiente operacional, de modo a garantir a continuidade da prestação dos serviços de TI.

Já as aquisições voltadas para o investimento envolvem geralmente investimentos em infraestrutura de TI, como compras de novos equipamentos, microcomputadores, servidores de dados, contratação de serviços de comunicação de dados ou de telecomunicação, etc., necessários para manter o parque computacional atualizado e em condições de responder às demandas dos serviços de TI.

Colocados desta forma, o contexto parece auspicioso em termos de direcionamento dos gastos, uma vez que a prioridade do gasto foi o investimento em detrimento ao custeio, seja dentro da vigência de cada PDTI, seja nas contratações aprovadas pelo CETI, seja no computo geral. De fato, isto é algo a comemorar, na medida em que gastos com investimento, além de estratégicos, envolvem ativos duradouros que contribuem para a sustentabilidade, mas há outros aspectos que merecem reflexão.

Embora investir na atualização do parque computacional, que é basicamente o que compõem as aquisições classificadas como investimento, seja algo mandatório e desejável, pois garante a continuidade da prestação dos serviços de TI em níveis desejáveis, este fato, por si só, não se constitui como um diferencial no sentido de um avanço tecnológico.

Ressente-se, por exemplo, de contratações de ferramentas ou *softwares* voltados para a modernização dos processos de trabalho ou para a melhoria da produtividade, tanto na área de infraestrutura de TI, quanto na área de desenvolvimento e manutenção de *software*, treinamento e qualificação dos técnicos de TI, investimento em novas tecnologias e inovação, dentre outros aspectos. Uma análise mais detalhada de cada PDTI, exposta a seguir, poderá corroborar esse raciocínio.

PDTI 2015-2018

A propósito dessas considerações, vale a pena citar as metas definidas pelo PDTI 2015-2018, em seu item 11.2 Necessidades Identificadas:

Quadro 5 - Critérios Matriz GUT

ID	Tipo	Descrição	G	U	T	GUT	Alinhamento
NC01	SISTEMAS	Aperfeiçoamento e manutenção dos sistemas de informação utilizados na CONAB de forma oportuna	3	3	3	27	
NC02	SISTEMAS	Melhoria da informatização, integração e automatização de processos e atividades da CONAB	4	4	3	48	Prover a

NC03	INFRAESTRUTURA	Disponibilização de equipamentos e serviços de TI atualizados e adequados aos usuários	4	3	3	36	Companhia de Infraestrutura de TI atualizada
NC04	PROCESSO	Aprimoramento da gestão dos processos internos e dos serviços prestados pela TI	3	2	2	12	
NC05	PESSOAS	Retenção, ampliação e capacitação do quadro de pessoal da TI da CONAB	3	3	2	18	

Fonte: PDTI 2015=2018

A tabela expressa as necessidades identificadas pelo referido PDTI, classificadas em termos da Matriz GUT[9]. Observe-se que a dimensão Sistemas NC02 obteve a maior pontuação (48), seguida pela dimensão Infraestrutura – NC03 (36).

A dimensão NC02 está associada a atividade fim da Sutin, os seja, às entregas finais da Sutin à Companhia, enquanto as restantes estão associadas às suas atividades meio (melhoria de processos internos, pessoas, etc.). Nesse sentido, a priorização das necessidades parece ser coerente.

A partir destas necessidades, o referido PDTI preparou seu Plano de Metas, por meio da definição de 11 metas, associando-as às necessidades identificadas. Dentre elas, destaca-se a meta MT05 (Manter 90% da infraestrutura de TI atualizada e com suporte vigente), associada à necessidade NC03. Com base no Plano de Metas, o PDTI apresentou seu Plano de Ação, com previsão de 29 ações para fazer frente às 11 metas definidas. O destaque fica para a ação AC14: Formalizar o processo de atualização da infraestrutura, baseada na meta MT05.

Ocorre que, examinando a Proposta Orçamentária do PDTI para 2015 e 2016, seja para custeio ou investimento, é possível concluir que ela é quase toda focada em investimentos voltados para a atualização e manutenção da infraestrutura, refletindo apenas uma das necessidades definidas (NC03) e uma das metas (MT05), que se refere a “Manter 90% da infraestrutura de TI atualizada e com suporte vigente”.

Os dados referentes às aquisições e contratações de TI para o período, que são basicamente relativas à Infraestrutura de TI, estão coerentes com os planos de investimentos, mas questiona-se por que as outras dimensões foram negligenciadas em termos de investimentos; em que pese a Estrutura COSO IC-IF 2013 (p. 105) dispor que para operar, a tecnologia

9 GUT, sigla para Gravidade, Urgência e Tendência, é uma ferramenta utilizada na priorização das estratégias, tomadas de decisão e solução de problemas de organizações / projetos.

demanda uma infraestrutura adequada, que varia de redes de comunicação para conectar tecnologias entre si e com o restante da entidade, passando por recursos computacionais para operar aplicativos, até a eletricidade, na esteira do item 82 do anexo à IN SFC/CGU nº 3, de 09/06/2017.

PDTIC 2021-2024

Este PDTIC também fez um levantamento das necessidades, totalizadas em 29, avaliando-as e classificando-as, pelo método GUT. Apesar de utilizar o mesmo método de classificação, esta relação de necessidades foi mais detalhada, envolvendo tanto as necessidades internas da Sutin quanto as demandas por serviços de TI da Companhia.

As 29 necessidades identificadas foram segmentadas em 4 grupos de ações: 1) suporte técnico (5 ações); 2) desenvolvimento de *software* (20 ações, correspondentes às demandas da Companhia por sistemas informatizados); 3) infraestrutura (20 ações relativas à infraestrutura) e Gestão de TI (17 ações).

Em termos do perfil das ações, o PDTIC 2021-2024 apresenta inovações em relação ao PDTI anterior[10]. Destaques para todo o grupo de ações referentes à gestão de TI, inexistente no anterior, e ao grupo de infraestrutura, que além de contemplar a renovação do parque tecnológico, incluiu também propostas diferenciadas, associadas à necessidade de fornecimento de soluções de Proteção e Segurança de Tecnologia da Informação (N1) [11], tais como:

> AC27 Elaborar processo de contratação de solução de TI de Data Loss Prevention - DLP.
>
> AC28 Desenvolver projeto para elaboração de norma e formalização de Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR.
>
> AC29 Desenvolver projeto para adoção de modelo de maturidade em Segurança de Tecnologia da Informação.

10 Mudanças a partir de um problema na tecnologia que precisa ser corrigido ou de uma solicitação da comunidade de usuários da Companhia (c.f. Estrutura COSO IC-IF 2013, p. 106).

11 Nos dias atuais, ameaças externas pairam os ambientes de negócios interconectados, exigindo esforços continuados para abordar os riscos associados (cfe. Estrutura COSO IC-IF 2013, p. 105).

AC30 Desenvolver projeto para implantação de Security Information and Event Management - SIEM.

Ou a ações referentes à necessidade "Prover soluções de infraestrutura em Nuvem" (N9), como:

AC32 Elaborar processo de contratação de gerenciamento/orquestramento de infraestrutura em nuvem.

AC33 Elaborar processo de contratação de infraestrutura e serviços de centro de dados em nuvem.

Entretanto, as contratações realizadas com base no PDTIC 2021-2024 não refletem estas inovações, continuando concentradas na atualização do parque tecnológico.

A previsão das ações AC32 e AC33, referentes à previsão da contratação de infraestrutura e serviços de centro de dados em nuvem, previstas no PDTIC 2021-2024, merecem uma reflexão.

Ocorre que a implementação dessas duas ações implica uma mudança de paradigma, no sentido da adoção de um novo modelo de prestação de serviços de TI. Um modelo de prestação de serviços de TI é uma decisão estratégica definida por uma organização para o provimento desses serviços, a exigir novos controles gerais de tecnologia, inclusive, na medida em que se alterem a infraestrutura de tecnologia, o gerenciamento da segurança e a aquisição, o desenvolvimento e a manutenção da tecnologia[12], na via de consequência.

Esta mudança, se implementada, vai ao encontro de nova tendência denominada "Computação em Nuvem"[13], já adotadas por órgãos da Administração Pública Federal (APF). Entretanto, é preciso salientar que se trata de uma mudança conceitual significativa para a prestação dos Serviços de TI e implicará uma completa revisão da visão e da alocação dos investimentos em ativos de TI. O tema mereceria uma abordagem mais aprofundada, inclusive

12 Estrutura COSO IC-IF 2013, p. 104.

13 Computação em Nuvem ou Nuvem Computacional é um modelo de computação em que todos os recursos (servidores, redes, aplicações e outros elementos relacionados a data centers) são disponibilizados para a TI e para os usuários finais por meio da internet, de maneira que a TI compra somente o tipo e a quantidade de serviços computacionais que realmente são consumidos. Extraído do artigo "Cloud Computing Definitions and Solutions", disponível em "https://www.cio.com/article/278067/cloud-computing-cloud-computing-definitions-and-solutions.html "

no tocante ao gerenciamento de novos riscos associados[14], mas infelizmente foge ao escopo desta auditoria.

Desta forma, conforme a análise dos dois PDTI, temos em ambos, a preocupação com o levantamento das necessidades da Companhia em termos de demandas por TI e com a melhorias dos processos internos da Sutin. A partir destas necessidades, ambos os instrumentos tiveram a preocupação de traduzir as necessidades em planos de ações, com a definição e priorização das ações a serem realizadas durante a vigência do instrumento de planejamento.

Entretanto, percebe-se que quando da elaboração dos orçamentos de TI para estes instrumentos (vide Anexo I, com os orçamentos transcritos), estes orçamentos não conseguem refletir os planos de ação, ficando concentrados nas ações que envolvam aquisições ou contratações referentes à atualização da infraestrutura de TI, isto é, na atualização do parque tecnológico. Esta atualização é mandatória e sua importância resta incontroversa, mas o que se questiona é a não contemplação dos demais itens dos planos de ação nestes orçamentos.

Os planos orçamentários previstos nos instrumentos de Planejamento objetivam realizar um registro da estimativa dos recursos orçamentários necessários, classificados entre investimento e custeio, para a execução das ações planejadas, uma vez que, como bem ressalta o PDTIC 2021-2025:

> *O plano orçamentário não é um artefato de proposta orçamentária da Companhia contendo todos os detalhamentos e classificações possíveis, mas, reúne a base das informações necessárias para se confeccionar uma proposta orçamentária. Um bom planejamento orçamentário com estimativas consistentes de custo pode ser um importante instrumento para obtenção dos recursos necessários à execução do PDTIC.*

Na prática, como demostra o Anexo II – Aquisições de bens e Serviços de TI - 2015-2023, as aquisições realizadas foram baseadas nestes orçamentos, e tem se concentrado na atualização do parque tecnológico.

14 Sempre que a inovação for introduzida, as respostas ao risco e as ações da gestão talvez precisem ser modificadas (cfe. COSO ERM 2017, p. 97).

4.2.2 Investimentos por Instâncias de aprovação das contratações (PDTI ou CETI)

A propósito das contratações de tecnologia da Informação, o REGULAMENTO DE LICITAÇÕES E CONTRATOS DA CONAB (RLC) (NOC 10.901) dispõe:

> ***Art. 596*** *As contratações de Tecnologia da Informação deverão, obrigatoriamente, estar previstas no Plano Diretor de Tecnologia da Informação (PDTI).*
>
> ***Parágrafo Único*** *- As contratações eventualmente não previstas no PDTI deverão ser previamente aprovadas pelo Comitê Executivo de Tecnologia da Informação (CETI).*

De forma explicita, o RLC traz a obrigatoriedade de as contratações de TI estarem previstas no PDTI como regra[15], e abre no seu parágrafo único uma exceção, que é a aprovação pelo CETI, em caso de contratações não previstas no PDTI.

No caso das contratações realizadas no período analisado (2015-2023), apresentadas no Anexo II, após a consolidação dos dados, temos o seguinte perfil:

Quadro 6 – Contratações por instância de aprovação

Instância de Aprovação		
PDTI	53	81,54%
Ceti	9	13,85%
Consad	1	1,54%
Não informado	2	3,08%
Total	65	100,00%

Fonte: Audin a partir dos dados da Sutin

Quadro 7 – Valores investidos por instância de aprovação

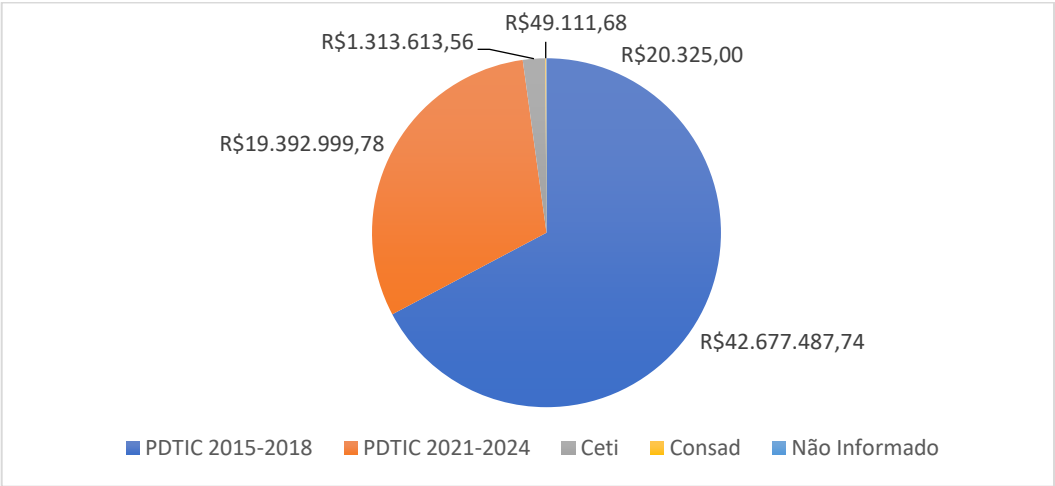
Instância	Valores	%
PDTIC 2015-2018	R$42.677.487,74	67,26%
PDTIC 2021-2024	R$19.392.999,78	30,56%
Ceti	R$1.313.613,56	2,07%
Consad	R$49.111,68	0,08%
Não informado	R$20.325,00	0,03%
Total	**R$63.453.537,76**	**100,00%**

Fonte: Audin a partir dos dados da Sutin

15 A autoridade deve ser delegada e a responsabilidade ser atribuída preferencialmente para profissionais que (i) demonstrem competência técnica para tomar decisões adequadas; (ii) respeitem, de forma consistente, as normas de conduta, as políticas e os procedimentos da organização; e (iii) que entendam as consequências dos riscos que assumem (cfe. COSO IC-IF 2013, p. 54).

Conforme Quadro 6, o PDTIC 2015-2018 foi responsável por 67,26 % dos investimentos realizados no período analisado (2015-2024), correspondendo a R$42.677.487,74. Importa ressaltar que se trata de valores à época, portanto, sem correção.

Gráfico 2 - Valores investidos por instância de aprovação



Fonte: elaborado por Audin

Verificou-se uma contratação que descumpriu o disposto no Art. 596 do RLC, no que tange à instância de aprovação. Trata-se da contratação por meio de ordem de Compra (OC 011/2019), cuja instância de aprovação foi o Consad, conforme o extrato das informações prestadas pela Sutin (vide AnexoII):

Ano	Contrato	Objeto	Inicio	Fim	Valor	Origem da aprovação	Observação
2019	OC 011/2019	Aquisição de 8 notebooks para CONSAD	02/25/2019	02/25/2020	R$ 49.111,68	CONSAD	

Além disso, verifica-se duas contratações referentes a cilindros para impressoras, cujas instâncias de aprovação não foram informadas (contrato 051 e OC 042/2020, cujo extrato das informações prestadas pela Sutin (vide Anexo II) é apresentado a seguir. De se observar que os valores são pequenos.

Ano	Contrato	Objeto	Inicio	Fim	Valor	Origem da aprovação	Observação
2019	051	Aquisição de 48 cilindros Drum Okidata para impressoras OKIDATA modelo OKI MB491+ e OKI B431dn.	12/11/2019	12/11/2020	R$ 15.000,00		Contrato simplificado 051/2019
2020	OC 042/2020	Aquisição de 25 cilindros para impressoras OKIDATA modelo OKI MB491+ e OKI B431dn.	09/24/2020	09/24/2021	R$ 5.325,00		Ordem de Compra 042/2020 - Valor: 5.325,00

Durante a reunião de busca conjunta de soluções, a Sutin informou que essas contratações se referem a material de consumo e foram erroneamente informadas como investimento.

O restante das contratações está aderente ao Art. 596 do RLC. As aquisições possuem o seguinte perfil: 81,54% foram realizadas com base PDTI, e 13,87% via CETI. A predominância de aquisições via PDTI, vai ao encontro do Art. 596 do RLC, que colocou a previsão via PDTI como regra e a aprovação via CETI como exceção.

Além deste aspecto quantitativo, o Quadro 2 nos informa que, num ranqueamento das maiores aquisições por valor investido, todas as grandes aquisições acima de 900 mil reais foram feitas tomando como base as indicações dos instrumentos de planejamento de TI. Já o Quadro 6 nos informa que a maioria das aquisições em termos de valores também foi realizada com base nos PDTIs.

Tais informações reafirmam a importância do PDTI como instrumento de planejamento das aquisições de Tecnologia da Informação, indicando que aquisições não programadas ocorram apenas em situação de excepcionalidade, sob a responsabilidade de quem competente tecnicamente e detentor de autoridade formal para fazê-lo[16].

4.3 Conclusão

Com base na exposição anterior, temos a seguinte síntese dos achados:

I. Há compras realizadas em 2019-2020, referentes ao PDTI 2015-2018 (contratos 8, 11 e 5). Isto é razoável, pois refere-se a um período em que não havia PDTI vigente (vigência havia se expirado em 2018). Ademais, o período coincide com a pandemia de Covid 19, no qual a Conab, como de resto toda a Administração Pública, se encontrava em situação emergencial.
II. Há aquisições aprovadas pelo Consad (OC 011/2019). De acordo com o RLC, Art. 596 e Parágrafo único, as compras deverão estar previstas no PDTI ou aprovadas pelo CETI, sob a égide da recomendável competência técnica para conduzi-las.
III. Os Termos aditivos celebrados sob vigência do PDTIC 2021-2024 se referem a contratos celebrados no PDTI anterior.

16 Cf. Estrutura COSO IC-IF 2013, p. 107, relativamente ao ponto de foco “realizar recorrendo a pessoal competente”.

IV. As aquisições são: 81,54% via PDTI, 13,87% via CETI, a predominância de aquisições via PDTI vai ao encontro da necessidade de estar em *compliance* com o normativo pertinente que, conforme Art. 596 do RLC, colocou a previsão via PDTI como regra e a aprovação via CETI como única exceção. Além disso, reafirma a importância do PDTI como instrumento de planejamento de aquisições.

V. Nas compras de cilindros (contrato 051, e OC 042/2020), não há referência à instância de aprovação, representando fragilidade nos controles internos da gestão, na medida em que houve atenção da gestão quanto a responsabilidades[17].

VI. Na análise temporal, os investimentos em Reais foram maiores no período 2015-2018 (R$ 36.220.710,66, correspondendo a 57% do total investido) que os anos posteriores, referente ao período 2015-2013 (27.232.827,10 correspondendo a 43%).

VII. Num ranqueamento das aquisições com valor acima de 900 mil reais, as 13 aquisições realizadas foram feitas com base em instrumento de planejamento (PDTIs).

VIII. Em relação à natureza das aquisições de TI, há o predomínio das aquisições voltadas para investimentos (85,22%) em relação ao custeio (14,78%), no total. A situação se mantém também dentro de cada instrumento de planejamento.

IX. Os dois PDTIs analisados (PDTI 2015-2018 e PDTIC 2021-2024) tiveram a preocupação de traduzir as necessidades da Companhia em termos de demandas de TI em planos de ações, com a priorização das ações a serem realizadas durante a vigência do instrumento de planejamento. Entretanto, os orçamentos de TI definidos para estes instrumentos não conseguem refletir os planos de ação priorizados, ficando concentrados nas ações que envolvam aquisições ou contratações referentes à atualização da infraestrutura de TI, isto é, na atualização do parque tecnológico. A necessidade desta atualização é incontroversa, mas o que se questiona é a não contemplação dos demais itens dos planos de ação nestes orçamentos. Na prática, as aquisições de bens e serviços de TI realizadas entre 2015-2023 foram baseadas nestes orçamentos e ficaram concentradas na atualização do parque tecnológico.

17 Independente da estrutura da organização, de definições de autoridade e responsabilidade, as linhas de subordinação e os canais de comunicação devem ser claros, no intuito de facilitar a prestação de contas nas unidades operacionais e áreas funcionais, sob a égide da accountability (cfe. Estrutura COSO IC-IF 2013, p. 53).

À luz dos achados de auditoria sumarizados acima, sugere-se:

I. que a Sutin observe o cumprimento do Art. 596 do RLC quanto à instância de aprovação das aquisições; e

II. avaliar a conveniência e oportunidade de, quando da elaboração dos PDTIs, nos itens referentes ao Planos de investimento e Custeio, comtemplar com recursos orçamentários outros itens além daqueles referentes a aquisições e contratações, considerando ações priorizadas nas matrizes GUT dos referidos instrumentos de Planejamento.

4.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

Nos últimos anos a Sutin enfrentou restrições orçamentárias que limitaram os investimentos em tecnologia da informação. O cenário tende a mudar, uma vez que a SUTIN passou a possuir rubrica específica destinada à área de TI em 2024. Isso representa um avanço significativo, pois permitirá direcionar recursos de forma mais eficaz para atender às necessidades de infraestrutura e ferramentas tecnológicas da Conab. Mesmo com as restrições orçamentárias enfrentadas nos últimos anos, a SUTIN conseguiu realizar compras pontuais, algumas por dispensa de licitação, para atender às necessidades imediatas da Companhia. Essas aquisições foram feitas de forma criteriosa, priorizando os recursos essenciais para manter a operação e garantir a continuidade dos serviços. Com a nova rubrica específica para a área de TI, poderemos não apenas manter, mas também expandir nossos investimentos de forma mais planejada e estratégica, visando melhorias contínuas na infraestrutura tecnológica da Conab.

1 - Foram realizadas compras de insumos de impressoras, entretanto devido à ausência de garantia contratual das impressoras, esses suprimentos são apenas compatíveis com os originais, mas com qualidade inferior. Isso pode resultar em efeitos colaterais na impressão e no funcionamento das impressoras. Consequentemente, os usuários expressam insatisfação durante a execução de suas atividades, seja devido a interrupções do serviço ou à necessidade de substituição dos suprimentos.

2 - Foi realizado a contratação de 10 licenças da plataforma Zoom, para permitir a realização de reuniões virtuais com o suporte necessário às atividades da companhia, contribuindo com a segurança e guarda das imagens/áudio.

3 - Foi realizada a contratação e o custeio de empresa para fornecer mão de obra para manter os computadores e impressoras, ambos sem garantia oficial dos fabricantes, operantes. Essa empresa era responsável por dar manutenção física e manter os equipamentos operacionais durante a duração do contrato.

4 - Está em curso um processo para a renovação do parque computacional; um processo para contratação do outsourcing de impressão; e para atender à crescente demanda por contratações de ferramentas e softwares voltados para a modernização dos processos de trabalho e para a melhoria da produtividade, a GESUT está com processo SEI para a aquisição de ferramenta de SUITE de escritório, incluindo ferramentas de escritório, e-mail e nuvem.

5 Análise do Risco 3 - Perda ou Indisponibilidade de back-up para recuperação de dados

5.1 Apresentação do Risco

A perda ou Indisponibilidade de *backup* para recuperação de dados pode comprometer o processo de Disponibilidade de Serviços de TI, e ter impacto no seu objetivo específico "Definir, documentar, instituir e normatizar os processos envolvendo a disponibilidade dos serviços de TI".

Caso materializado o risco, podemos ter como consequências dificuldade ou impossibilidade de voltar a posição de algum arquivo ou um servidor ou, até mesmo, o comprometimento das rotinas de recuperação em caso de desastres e falhas. Enfim, pode comprometer a segurança da prestação dos serviços de TI, como um todo.

Com vistas a avaliar este risco, foi formulada a seguinte questão de auditoria:

> "Quais os principais problemas associados à execução das rotinas de segurança (*backup*) no ambiente de TI da Conab e suas consequências? ".

5.2 Análise do Risco

Com vistas a prover subsídios para responder à citada questão proposta, a análise do risco foi realizada sob pontos sensíveis, como a questão da adoção de uma política de arquivamento, da inexistência de um processo de *backup* formalmente definido e normatizado e, por fim, foi realizada uma avaliação da adoção de boas práticas relativa ao tema, na Conab.

5.2.1. Definição de uma política de arquivamento de dados

Indagada sobre quais os principais problemas encontrados pela Sutin para a execução dos procedimentos de *backup*, recuperação e armazenamento e as sugestões/oportunidades de melhoria, esta respondeu que

> *Além da ausência de uma norma de backup, a principal dificuldade encontrada pela GEASI no processo de backup está relacionada a ausência de uma política de arquivamento efetiva, que permita o arquivamento de dados que necessitem de guarda a longo prazo e o descarte de dados desnecessários. Devido a essa ausência, há um crescimento constante no*

> *volume de dados, não sendo possível realizar expansões de capacidade do sistema capazes de acomodar o crescimento.*

Assiste razão à Sutin. Uma política de arquivamento efetiva, se definida e implantada, teria um forte impacto na execução do processo de *backup*, possibilitando a classificação e priorização de quais arquivos realmente precisam constar no *backup*, tornando-o mais eficiente pela redução do volume de dados a serem salvos. As consequências seriam a economia de tempo de processamento dos *backups* e de recursos físicos demandados, como fitas.

A questão do volume de dados a serem salvos pelas rotinas de *backup* é relevante, seja pelo volume em si, atualmente estamos falando de cerca de 26,84 terabytes (TB)[18] [19], seja pela sua taxa de crescimento; o volume de dados a serem salvos cresceu 150,12 % nos últimos 7 anos, ficando a média anual em torno de 21,45 % ao ano, se fizermos um exercício de proporcionalidade[20].

Com esta média, o volume total pode dobrar a cada 4 anos. Considere-se, também, que o tempo médio de realização de um *backup* completo (*backup full*) fica em torno de 52 horas. Ou seja, se nada for feito, a tendência é o crescimento fora do controle do volume de dados a serem copiados, tornando o problema cada vez mais crítico.

A adoção de uma política de arquivamento requer a necessidade de definição, por parte do negócio, da temporalidade das informações, ou seja, por quanto tempo a Sutin deve manter cópia de segurança das informações, em observância a requisitos legais e normativos.

O foco desta política poderia ser as informações de arquivos mantidos pelas áreas da Companhia nos servidores da Sutin, e não nos bancos de dados mantidos pelos sistemas informatizados. Esta escolha, segundo a Sutin, justifica-se porque os bancos de dados armazenam dados estruturados, basicamente do tipo texto, com tamanho predefinido e, consequentemente, com crescimento mais previsível e estável, enquanto os dados do usuário

---

18 O terabyte é um múltiplo do byte, que, atua como indicador de volume de armazenamento de dados em um dispositivo eletrônico. Sua abreviatura é TB, sendo que 1 TB equivale a:

- 1.024 gigabytes
- 1.048.576 megabytes.
- 1.099.511.627.776 bytes

19 Vide o quadro 10- Evolução do volume de dados envolvidos com backup, no item 5.2.2 deste relatório.

20 Vide o quadro 10- Evolução do volume de dados envolvidos com backup, no item 5.2.2 deste relatório.

podem crescer de forma descontrolada, já que o usuário pode armazenar diversos tipos de dados, como fotos de viagens, filmes, entre outros, e sem limites, pois não se verificou a existência de uma política de arquivamento.

Com a crescente digitalização das informações, as enormes pilhas de documentos em papel desapareceram das mesas e prateleiras das áreas, sendo transformadas em arquivos eletrônicos. Entretanto, o problema apenas foi transferido de lugar, pelo enorme quantitativo de arquivos em meio eletrônico a ser administrado pela Sutin, que é a responsável pela guarda destes.

Pode-se citar como exemplo os arquivos de documentos mantidos pela Gesas, que estão atualmente por volta de 700 gigabytes (GB), e com crescimento constante. Além do volume extenso de documentos antigos, o gestor da Geasi alerta para o fato de que estes arquivos são manuseados muitas vezes por terceirizados, como estagiários, com alta rotatividade e sem necessariamente consciência da necessidade do sigilo, transformando-se num risco para a Companhia, à vista da Lei nº 13.709, de 14/08/2018, inclusive. A Proge também mantém um acervo considerável de documentos na Sutin, de certa de 1 terabyte (TB), e a área de fiscalização cerca de 400 GB de arquivos. Esses são alguns exemplos; há naturalmente outras áreas com o mesmo problema.

Trata-se de um desafio que transcende às competências da Sutin, uma vez que cabe ao negócio definir a temporalidade de suas informações; sem embargos a que informações sejam classificadas mediante uso de categorias (por áreas funcionais, por riscos estratégicos, etc.), no intuito de ajudar a Companhia a melhor agregar informações, sob a égide da gestão de dados[21].

Consultando o Regimento Interno da Companhia (NOC 10.104) acerca de competências associadas à questão apontada, temos que:

> *Art. 94. À Gerência de Material, Arquivo e Protocolo (Gemap), subordinada à Superintendência de Administração, compete*
>
> *VII - acompanhar, controlar, orientar e fiscalizar as atividades relacionadas ao arquivo permanente da Companhia, cumprindo e fazendo cumprir os normativos internos e legislação vigente*

21 Na esteira do COSO ERM 2017, p. 107.

> *Art. 150. À Comissão Permanente de Avaliação de Documentos, vinculada à Diretoria*
>
> *Administrativa, Financeira e de Fiscalização, compete:*
>
> *I - adaptar e orientar a aplicação do código de classificação de documentos e da tabela de temporalidade e destinação de documentos de arquivos relativos às atividades-meio da Administração Pública, aprovados pelo Conselho Nacional de Arquivos (Conarq)*
>
> *II - elaborar o código de classificação de documentos e a tabela de temporalidade de documentos relativos às atividades-fim;*
>
> *Art. 143. À Comissão Permanente de Avaliação de Documentos Sigilosos (Cpads), vinculada à Diretoria Administrativa, Financeira e de Fiscalização, compete:*
>
> *V - elaborar a tabela de temporalidade de guarda dos documentos.*

Por meio da Solicitação de Auditoria nº 15, encaminhada à Diafi, obteve-se informações acerca da situação das duas comissões citadas: Comissão Permanente de Avaliação de Documentos (CPAD) e Comissão Permanente de Avaliação de Documentos Sigilosos (Cpads). Ambas as comissões se encontram ativas, com composição definida:

> *A CPAD foi constituída por meio da Portaria Presi nº 037/2014 (alterada pela Portaria Presi nº 055/2020) sei nº 30999558 e possui 10 membros em sua composição. Importante destacar que 2 membros solicitaram desligamento, portanto, a CPAD contará com atualização futuramente.*
>
> *A CPADS foi constituída por meio da Portaria Presi nº 213/2017 (alterada pelas Portarias Presi nºs 264/2017 e 316/2019) Sei nº 31001551, 31002130 e 31002193 e possui 10 membros em sua composição*

A CPAD informa, ainda, que "elaborou um Termo de Referência visando a contratação de empresa especializada em Gestão Documental para subsidiar a Conab na elaboração dos instrumentos arquivísticos - Código de Classificação e Tabela de Temporalidade de Documentos relativos às atividades-fim da Companhia".

Os artigos 143 e 150 do Regimento Interno delegam à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) e a Comissão Permanente de Avaliação de Documentos (CPAD) competências de tratar de questões associadas à temporalidade de documentos. Entretanto, não há referência nestes artigos às informações que estão sob a guarda da Sutin, configurando-se um aparente vácuo normativo.

Ocorre que, estas informações são oriundas ou derivadas destes documentos, de que tratam os artigos 150 e 143, *vide* o processo de digitalização mencionado, devendo, portanto, serem tratadas pelas comissões CPAD e CPADS, por analogia.

Vale a pena reproduzir como o documento de *backup* da Geasi trata o tema: “Ressalta-se que, a definição do escopo e dos prazos de arquivamento dos dados institucionais da Conab deverá ser objeto de estudo e definição em norma específica, uma vez que envolve a classificação dos dados institucionais à luz do que estabelece o código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal”.

Questionada sobre as tratativas já realizadas para discutir a questão da definição da temporalidade dos dados do negócio sob sua guarda, com as áreas da Companhia, a Sutin informou que: “Até o momento foram feitas apenas tratativas informais junto as áreas de gestão documental, como a GEMAP”.

Por fim, quando da definição da política de arquivamento de dados, sugere-se que a Sutin considere as seguintes medidas do “Controle 03 - Proteção de dados”, do Relatório CIS 8, cujo objetivo é “Desenvolver processos e controles técnicos para identificar, classificar, manusear com segurança, reter e descartar dados. ”

> ***3.5 descartar dados com segurança***
>
> *Descarte os dados com segurança conforme descrito no processo de gestão de dados da empresa. Certifique-se de que o processo e o método de descarte sejam compatíveis com a sensibilidade dos dados.*
>
> ***3.7 estabelecer e manter um esquema de classificação de dados***
>
> *Estabeleça e mantenha um esquema geral de classificação de dados para a empresa. As empresas podem usar rótulos, como “Sensível”, “Confidencial” e “Público”, e classificar seus dados de acordo com esses rótulos. Revise e atualize o esquema de classificação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.*

5.2.2. Inexistência de política ou norma para o processo de *backup*

A preocupação com segurança dos procedimentos de *backup* na Sutin na Conab não é recente. Já em 2021, a questão surgiu na NOTA TÉCNICA GENOP SEI N.º 2/2021, por conta de demanda à Audin (então Auger) para análise de resposta da Sutin ao OFÍCIO INTERNO AUGER SEI N.º 12864359/2020, que solicitava “informar quais as medidas de segurança que são

adotadas para mitigar os riscos de acesso indevido aos dados da Conab" [22]. A referida resposta da Sutin veio por meio do Despacho Geasi SEI nº13090550, que utilizou como referência as recomendações do Centro de Tratamento de Incidentes e Resposta - CTIR Gov - para mitigar o risco a ameaças.

Transcreve-se trecho da referida Nota Técnica:

> *Resposta da Sutin à recomendação "8. (CRÍTICA) Revisar as políticas de backups dos principais sistemas e base de dados, inclusive testar uma amostragem de backup e garantir que a restauração está em conformidade" [23] suscita especial atenção. Para este item, a Sutin respondeu:*
>
> *Em execução**. Embora a Conab não tenha exatamente uma política de backup institucionalizada**, esta GEASI executa o backup corporativo de sistemas e base de dados, com retenção e recuperação, **dentro dos limites dos recursos tecnológicos disponíveis e baseado em acordos informais realizados anteriormente**. Esse plano de backup, recuperação e retenção está sendo melhor documentado nesta oportunidade**. <grifo nosso>*

No âmbito desta auditoria, questionada acerca da existência de um processo de *backup* definido e normatizado, a Sutin respondeu: "Não possuímos no momento uma norma que trate dos processos de *backup*, com um projeto para formalização de tal norma proposto como atividade no próximo semestre para o plano de trabalho da gerência (10/2023 a 04/2024) ".

Segundo a Geasi, os procedimentos de *backup* são executados consoante o que estabelece o documento de *backup* disponível no repositório geasiwiki[24], por não existir uma política corporativa aprovada. O referido documento detalha, ao longo dos seus itens os conceitos e procedimentos envolvido com as rotinas de extração, recuperação e arquivamento de *backup* na Sutin.

---

22 No tocante às atividades de controle, a restrição de acesso deve ser uma considerada na maioria dos processos de internos de trabalho e é frequentemente incluída como um objetivo do processamento de informações, pois sem a restrição adequada de acesso às transações, em um processo de negócios, as atividades de controle na organização podem ser burladas (cfe. Estrutura COSO IC-IF 2013, p. 97, c/c o item 82 do anexo à IN SFC/CGU nº 3, de 09/06/2017).

23 Tratava-se de uma das recomendações do Centro de Tratamento de Incidentes e Resposta - CTIR Gov - para mitigar o risco de ameaças extraídas do Alerta Especial n° 07/2020, de 11 de novembro de 2020, do Gabinete de Segurança Institucional da Presidência da República e a situação de atendimento dessas recomendações na Companhia.

24 Geasiwiki é o nome de um ambiente específico da Geasi, em meio eletrônico, contendo os arquivos (páginas web), que são compartilhados pelos técnicos que tem acesso a ele. Trata-se de um ambiente de compartilhamento de informações e conhecimentos da Geasi.

Em síntese, segundo o referido documento de *backup*, os procedimentos[25] atuais são executados da seguinte forma:

Quadro 08 – Quadro resumo dos procedimentos de *backup* da Sutin

Periodicidade	Tipo de backup	Quando?	Duração	Retenção
Diário	Diferencial[26]	2 a 5 feira, às 20 h	14 h	1 semana
Semanal	Full	Às sextas, a partir das 20 h	52 h	No máximo 3 semanas
Mensal	Full	Às sextas, a partir das 20 h	52 h	No máximo 6 meses
Anual	Full	Às sextas, a partir das 20 h	52 h	No máximo 1 ano

Fonte: Audin, com base no documento de *Backup*.

Ainda segundo este documento, temos as definições dos tipos de *backup*:

> ***Backup Full***
>
> *Um Backup Full consiste na cópia de todos os dados que estão presentes nos caminhos definidos no conjunto de arquivos configurados, na confirmação da integridade dos dados por meio da checagem de cada um deles e, finalmente, no armazenamento de todos esses dados em fita.*
>
> ***Backup Diferencial***
>
> *Nessa modalidade, o serviço compara os atributos do último backup em modo full com o sistema de arquivos atual e realiza a cópia dos dados que foram modificados*

A propósito da execução dos procedimentos de *backup*, em entrevista, o gestor da Geasi informou que o processo é bastante automatizado, requerendo poucas intervenções manuais, quando tudo corre de maneira correta e usual.

Segundo a Sutin, "quanto ao *software* e *hardware* utilizados, ainda mantemos o uso do Bacula, com a biblioteca de fitas Oracle SL-150. O conjunto da solução permite a automação quase que total das atividades, sendo necessário apenas realizar a inserção e remoção de fitas. Como

25 No subitem 9.2.7 do Acórdão nº 3.384/2013-TCU-Plenário, a Corte de Contas explicita preocupação no sentido da formalização de rotinas de backup, a título de ilustração.

26 Em entrevista, o gestor da Geasi informou que o tipo de backup que é efetivamente executado na Sutin é o incremental e não o diferencial, conforme definido no documento de backup.

a garantia da biblioteca está próxima ao fim, foi instruído o processo 21200.005404/2020-65 para aquisição de novos equipamentos para substituição dos atuais".

O processo de *backup* é disparado automaticamente, de acordo com o agendamento prévio das tarefas (Jobs) e com a periodicidade definida, sendo executado em um dispositivo de *hardware* específico e gerenciado pelo *software* gerenciador de *backup* (Bacula).

Ao final do processamento do *backup*, o *software* Bacula gera um e-mail que é enviado ao analista responsável, com todas as informações do processamento, inclusive a lista dos arquivos salvos. Ao examinar este arquivo, caso tenha havido alguma falha na operação, o analista toma as providencias para que o processamento seja retomado para os arquivos que não foram salvos. Segundo o gestor da Geasi, a ocorrência de erros de processamento é incomum. Caso não haja erros, significa que o processo de *backups* foi gerado corretamente.

Visando assegurar o cumprimento da tarefa de conferência do processamento do *backup*, a Geasi desenvolveu e implementou uma camada adicional de controle, na qual, todos os dias, é aberto automaticamente um chamado no Sistema de Gestão de Demandas (SIGEDE), para o analista responsável pela conferência, para lembrá-lo de examinar o e-mail enviado pelo *software* gerenciador do *backup* com o resultado do processamento. Concluída a verificação, o analista registra as eventuais ocorrências na resposta do chamado.

Indagada sobre a guarda dos *logs* de processamento dos *backups* realizados e dos e-mails disparados, a Sutin informou que estes arquivos não vêm sendo armazenados, mas que é possível fazê-lo. A manutenção destes arquivos por uma periodicidade definida é importante porque permite recuperar o histórico das informações sobre o processamento dos *backups*, possibilitando auditorias futuras no processo, inclusive.

Quanto ao prazo de retenção das fitas[27], o gestor da Geasi informou que apesar do *software* Bacula ter capacidade para defini-lo de forma automática, esta tarefa é feita manualmente, pelo analista, em virtude da pouca disponibilidade de fitas. Diariamente, após a análise do

27 O prazo de retenção de uma fita backup é tempo que a fita estará disponível para o processo recuperação dos dados, quando demandado, uma vez que as fitas são reutilizadas. Este prazo é definido em função da quantidade de fitas disponíveis para o processo, ou seja, quanto menos fitas disponíveis, menor será o tempo de retenção.

processamento do *backup* corrente, o analista avalia se há fitas disponíveis para o próximo *backup*, e caso não haja, ele seleciona as fitas mais antigas.

Conforme se pode observar, o nível de automação do processo é relativamente alto, ficando para os analistas as apenas a tarefa de monitorar e conferir o resultado do processamento dos *backups* e selecionar as fitas para o próximo processamento. Entretanto, há necessidade de normatizar o processo, necessidade que a própria Sutin já reconheceu e informou ter planos de elaborá-lo no próximo semestre[28].

5.2.3. Evolução dos parâmetros referentes aos *Backups*

Quadro 09 –Quantitativo de fitas envolvidas com as operações de *backup* na Sutin

Item	Descrição	Situação em Abril/2021	Situação em Setembro/2023	Aumento	% Crescimento
Fitas	Total de fitas disponíveis na Sutin para a execução dos *backups*	118	136	18	15,25%

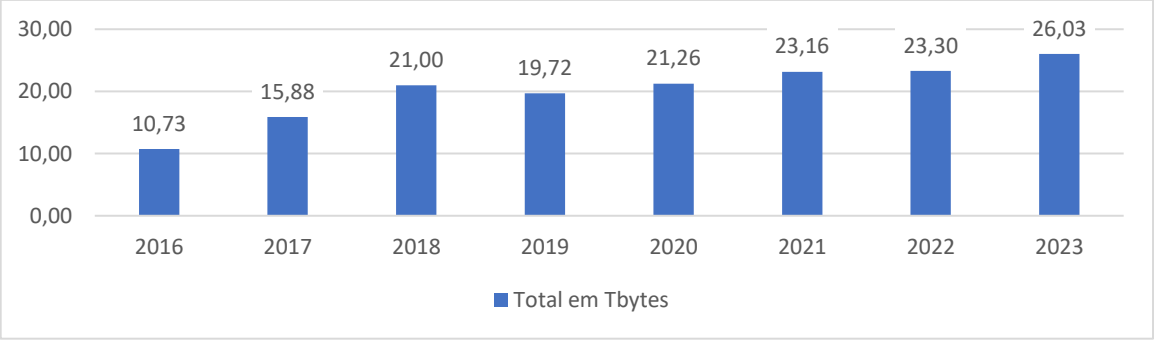
Fonte: Elaborado por Audin a partir de dados fornecidos pela Sutin.

Quadro 10 – Evolução do volume de dados envolvidos com *backup*

Ano	2016	2017	2018	2019	2020	2021	2022	2023
Total em Terabytes	10,73	15,88	21,00	19,72	21,26	23,16	23,30	26,84
Taxa de Crescimento (%)		47,98%	32,24%	-6,11%	7,84%	8,91%	0,62%	15,20%
Taxa de crescimento total	150,12%							
Taxa de crescimento média anual	21,45%							

Fonte: Sutin.

Gráfico 03 – Evolução do volume de dados envolvidos com *backup* (em TB)



Fonte: elaborado por Audin a partir de dados fornecidos pela Sutin

28 No subitem 9.1.10 do Acórdão nº 436/2008-TCU-Plenário, no subitem 9.4.17 do Acórdão nº 1.163/2008-TCU-Plenário e no subitem 9.2.24 do Acórdão nº 1.382/2009-TCU-Plenário, há referências da Corte de Contas ao COBIT 4.1, item DS11.5 - Backup e restauração, cujos procedimentos devem ser documentados e implementados, além de mencionar a necessidade de considerar armazenamento off-site para cópias de backup para proteção adicional, a título de ilustração.

Os dados do quadro 03 – Evolução do volume de dados envolvidos com *backup* – foram obtidos por meio da Solicitação de Auditoria nº 16, que requereu informações acerca da evolução, ao longo do tempo, do crescimento do volume de dados para a execução dos procedimentos de *backup*. Como resposta, a Sutin enviou a Planilha crescimento do *backup*, com os referidos dados.

Segundo a Sutin, os referidos dados "correspondem ao crescimento do volume do *backup*, estimado a partir dos *backups* anuais. O *backup* anual é um *backup full*, idêntico aos executados nos finais de semana, com a diferença de ser retido por mais tempo, para garantir-se o arquivamento de dados por longo prazo. Assim, esses *backups* funcionam como uma fotografia anual de nosso volume de dados de *backup full*.

Entre 2018 e 2019, houve uma redução no volume, pois se implementou uma política de tratar dados de compartilhamentos públicos como dados temporários, e, portanto, excluídos do *backup"*.

5.2.4. Avaliação do controle "Recuperação de Dados" e suas medidas

O Relatório de Controles CIS v8[29] foi utilizado como referência de boas práticas relativas ao risco em análise. O framework Center for Internet Security (CIS) prevê um total de dezoito controles críticos de segurança cibernética (SegCiber), subdivididos em 153 medidas de segurança, sendo que cada controle envolve um conjunto de medidas de segurança para sua avaliação.

Para o risco em análise, foi utilizado o controle 11 "Recuperação de Dados" que, segundo o Relatório, estabelece e mantém práticas de recuperação de dados suficientes para restaurar ativos corporativos dentro do escopo para um estado pré-incidente e confiável.

O Relatório de Controles CIS v8 foi o mesmo adotado como referência pelo Tribunal de Contas da União (TCU), para a geração do relatório **"**Acompanhamento de Controles Críticos de Segurança Cibernética das Organizações Públicas Federias", que tinha por objetivo avaliar a adoção, pelas organizações públicas federais, de controles e medidas consideradas críticas no

29 Trata-se do mesmo relatório utilizado pelo TCU para realizar a elaboração da pesquisa "Acompanhamento de Controles Críticos de Segurança Cibernética das Organizações Públicas federias", cujo resultado foi comentado na análise do risco 11.

contexto da segurança cibernética. Os dados deste relatório relativos à Conab, foram discutidos e avaliados quando da análise do risco 11 desta auditoria.

Desta forma, para a avaliação do controle em questão, recuperação de dados, procurou-se adotar o mesmo referencial teórico e a mesma forma de obtenção dos dados, ou seja, por meio de autoavaliação pela Sutin. A pesquisa foi realizada por meio da Solicitação de Auditoria nº 12.

A seguir, serão apresentados os resultados da pesquisa com vistas a conhecer a aderência dos procedimentos relativos às rotinas de segurança da Sutin às medidas previstas no controle 11 "Recuperação de Dados", do Relatório CIS. Para cada medida serão apresentadas sua descrição transcrita do Relatório, a situação de sua adoção na Sutin e as considerações da auditoria.

Medida: 11.1 Estabelecer e manter um processo de recuperação de dados

Descrição: Estabeleça e mantenha um processo de recuperação de dados. No processo, aborde o escopo das atividades de recuperação de dados, a priorização da recuperação e a segurança dos dados de *backup*. Revise e atualize a documentação anualmente ou quando ocorrerem mudanças significativas na empresa que possam impactar esta medida de segurança.

Resposta da Sutin: Adota parcialmente

> *Mantemos um processo de backup/recuperação que envolve todo o ciclo de vida dos servidores usados para tratamento de dados. Ao realizar a instalação de cada servidor, é criada automaticamente configuração junto ao serviço de backup, que normalmente é ajustada pelos administradores de rede para adequação aos serviços usados. O processo está documentado no geasiwiki, com revisões ocorrendo quando há alterações significativas no processo, entretanto não há norma formalizada ou "oversight" e indicadores sobre tal processo sendo levados à alta gestão ou comitê competente que a represente, por isso a adoção parcial do controle.*

Avaliação da Auditoria: Adota parcialmente.

A Sutin possui documento que detalha, ao longo dos seus itens, os conceitos e procedimentos envolvido com as rotinas de extração, recuperação e arquivamento de *backup*, localizados em repositório digital conhecido como "geasawiki".

Este documento define que “Recuperação de um *backup* é um processo em que, após um sinistro que ocasione em perda de dados, provocado por falha de equipamentos, *software* ou falha humana, dados previamente armazenados em mídia externa por meio de *backup* substituem os dados perdidos ou danificados. ”

Entretanto, o documento não especifica como devem ser os procedimentos de recuperação dos *backups*. Além disso, o documento está desatualizado, haja vista as atualizações presentes na resposta da SA nº 12.

A Sutin reconhece que o processo de *backup* não se encontra normatizado, razão razoável para ter avaliado como adoção parcial da medida, avaliação corroborada por esta auditoria.

Medida: 11.2 Executar *backups* automatizados de Dados

Execute *backups* automatizados de ativos corporativos dentro do escopo. Execute *backups* semanalmente ou com mais frequência, com base na sensibilidade dos dados.

Resposta da Sutin: Adota

> *O serviço de backup utiliza combinação de processo automático de produção de servidores com software (Bacula) e hardware (biblioteca de fitas), que permite a execução de processo automático de backups. O processo pode ser acompanhado pelo dashboard disponível em http://dfbsa80.conab.gov.br/bacula-web/ (acesso apenas disponível na rede interna).*

Considerações da Auditoria: Adota

O documento de *backup* especifica o tipo de *backup* realizado na Sutin e a periodicidade, conforme indicado no Quadro 08 – Quadro resumo dos procedimentos de *backup* da Sutin, do item 5.2.2 deste relatório.

Segundo o documento de *backup* “Para a guarda dos dados do *backup* é utilizado, como meio de armazenamento físico, fitas do tipo LTO6 em uma *tape library* da Oracle - a Oracle StorageTek SL150. Segundo a SA nº 12, “Quanto a guarda dos *backups*, os dados são armazenados em fitas magnéticas do tipo LTO-7”. Na avaliação desta auditoria, a medida é adotada na Sutin.

Medida: 11.3 Proteger os dados de recuperação Dados

Proteja os dados de recuperação com controles equivalentes dos dados originais. Referencie o uso de criptografia ou separação de dados, com base nos requisitos.

Resposta da Sutin: Adota.

> *Os dados de backup são separados por meio de filesets distintos, e armazenados em fitas. O acesso ao serviço de backup é restrito ao grupo de administradores da GEASI, e o acesso físico para as fitas que estão no equipamento de backup depende de acesso biométrico da sala-cofre e uso de senha para a biblioteca de fita. Para os dados semestrais, que são armazenados em cofre na matriz, é necessário acesso por senha. Na avaliação desta auditoria a medida é adotada na Sutin.*

Considerações da Auditoria: Adota

Medida: 11.4 Estabelecer e manter uma instância isolada de dados de recuperação

Estabeleça e mantenha uma instância isolada de dados de recuperação. Exemplos de implementações incluem controle de versão de destinos de *backup* por meio de sistemas ou serviços *online*, na nuvem ou fora do site local.

Resposta da Sutin: Adota.

> *Os dados de recuperação são mantidos em fitas, que são por sua natureza isolados e offline. Os dados são separados por jobs, garantindo o versionamento por data.*

Considerações da Auditoria: Não Adota

Na SA nº 12, a Sutin informa que "Quanto a guarda dos *backups*, os dados são armazenados em fitas magnéticas do tipo LTO-7, que ficam armazenadas dentro da biblioteca de fitas na sala-cofre da Matriz. Semestralmente, um conjunto de fitas, que representa o *backup* semestral, é movido para o cofre, localizado na Sutin. O tempo de retenção atual foi reduzido devido à ausência de fitas, ficando em três semanas.

Como a garantia da biblioteca está próxima ao fim, foi instruído o processo 21200.005404/2020-65 para aquisição de novos equipamentos para substituição dos atuais."

A guarda das fitas magnéticas na Sala Cofre e no Cofre da Sutin contraria a recomendação da medida que informa na sua descrição que "Exemplos de implementações incluem controle de versão de destinos de *backup* por meio de sistemas ou serviços *online*, **na nuvem ou fora do site local**." <grifo nosso>.

Por sua vez, a norma ABNT NBR ISO/IEC 17799, que trata da Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação, em seu item 10.5.1, letra d), informa que:

> 10.5.1 Cópias de segurança das informações
>
> Convém que os seguintes itens para a geração das cópias de segurança sejam considerados:
>
> d) as cópias de segurança sejam armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal;

A guarda dos *backups* nas instalações da Sutin, ainda que na sala cofre, pode representar um risco para o processo de recuperação. Basta pensar na ocorrência, eventual, mas não impossível, de algum desastre capaz de acometer as instalações da Sutin e do seu Data Center. Se este possível desastre vier a causar danos aos dados, provavelmente causarão também aos *backups*; sem embargos a outros possíveis fatores a exemplo de indícios de umidade no local, na esteira do subitem 1.8 do Acórdão nº 1.041/2009-TCU-Plenário, p.e. Na visão desta auditoria, considerando as recomendações de boas práticas citadas, esta medida não é adotada.

Medida: 11.5 Testar os dados de recuperação

Teste a recuperação do *backup* trimestralmente, ou com mais frequência, para uma amostra dos ativos corporativos dentro do escopo.

Situação da medida na Sutin: Não Adota

> *Os dados são testados por amostragem na execução dos jobs normais de recuperação. Não possuímos, ainda, dentro de nosso processo, uma validação periódica da recuperação fora destas solicitações de recuperação.*

Considerações da Auditoria: Não adota

O teste da recuperação do *backup* é muito importante, pois permite saber, por amostragem, se o *backup* foi gerado de forma íntegra e se seu processo de geração está funcionando corretamente.

Segundo o Relatório Cis 8, "uma vez por trimestre (ou sempre que um novo processo ou tecnologia de *backup* for introduzido), uma equipe de teste deve avaliar uma amostra aleatória

de *backups* e tentar restaurá-los em um ambiente de teste. Os backups restaurados devem ser verificados para garantir que o sistema operacional, a aplicação e dados do *backup* estejam intactos e funcionais".

Em entrevista, o gestor da Geasi esclareceu que o teste por amostragem a que se refere na resposta são as operações de recuperação de arquivos, quando demandados pelos usuários. O entendimento é que se esta recuperação é bem-sucedida, há evidência de que aquele *backup* estava integro e funcionando.

Entretanto, o gestor entende que este fato não é suficiente para demonstrar o atendimento da medida, razão pela qual avaliou como "não adota". Esta auditoria corrobora este entendimento de que a medida não é adotada na Sutin.

5.2.5 Síntese dos resultados da avaliação do Controle 11 – Recuperação de dados

Quadro 11 - Síntese dos resultados

Medida	Avaliação da Sutin	Avaliação da Auditoria
11.1 estabelecer e manter um processo de recuperação de dados	Adota parcialmente	Adota parcialmente
11.2 executar *backups* automatizados Dados	Adota	Adota
11.3 proteger os dados de recuperação Dados	Adota	Adota
11.4 estabelecer e manter uma instância isolada de dados de recuperação	Adota	Não adota
11.5 testar os dados de recuperação	Não adota	Não adota

Fonte: Audin

5.3 Conclusão

Com base na exposição anterior, temos a seguinte síntese dos achados:

I. A taxa de crescimento dos dados salvos nos *backups* nos últimos 7 anos foi de 150,12 %, ficando a média anual em torno de 21,45 % ao ano, se fizermos um exercício de proporcionalidade. Com esta média, o volume total pode dobrar a cada 4 anos[30].

30 O COSO ERM 2017 (p. 103) aborda o desafio às organizações hodiernas em face da enorme quantidade de dados e pela velocidade com a qual eles devem ser processados, organizados e armazenados, numa espécie de "sobrecarga de informações"; nesta ambiência, impõe-se o fornecimento de "informações certas, da forma correta, com o nível de detalhes correto, às pessoas certas e tempestivamente".

II. Não há uma política de arquivamento efetiva, adotada na Sutin, que permita o arquivamento de dados que necessitem de guarda a longo prazo e o descarte de dados desnecessários.

III. Os artigos 143 e 150 do Regimentos Interno delegam à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) e a Comissão Permanente de Avaliação de Documentos (CPAD) competências de tratar de questões associada à temporalidade de documentos. Entretanto, não há referência nestes artigos às informações que estão a guarda da Sutin, configurando-se um aparente vácuo normativo. Ocorre que, estas informações são oriundas ou derivadas destes documentos de que trata os artigos 150 e 143, vide o processo de digitalização mencionado, devendo, portanto, serem tratadas pelas comissões CPAD e CPADS, por analogia. A Situação atual destas comissões foi levantada e elas se encontram constituídas e ativas, ambas possuindo 10 membros em sua composição.

IV. Não há política ou norma específica para o processo de *backup*. O que existe é um documento residente no geasiwiki, que especifica os procedimentos de *backup*. Este documento está desatualizado. Por meio de levantamentos feitos em entrevista com o Gestor da Geasi, verificou-se que o processo de *backup* está definido, mas não está documentado e normatizado.

V. Não é realizada a guarda dos *logs* de processamento dos *backups* realizados e dos e-mails disparados. A Sutin informou que estes arquivos não vêm sendo armazenados, mas que é possível fazê-lo.

VI. A autoavaliação, feita pela Sutin, das medidas previstas no controle “Recuperação de dados”, do relatório Cis 8, indicou que, das 5 medidas previstas, a Sutin afirma adotar três medidas integralmente (medidas 11.2, 11,3 e 11,4), adotar uma medida parcialmente (11.1) e não adotar uma medida (11.5). Esta auditoria discorda, respeitosamente, da avaliação da medida 11.4. No entendimento desta auditoria, a medida 11.4 é não adotada e as demais avaliações foram ratificadas pela auditoria.

VII. A guarda das fitas magnéticas na Sala Cofre está em desacordo com a recomendação da medida 11.4 do relatório CIS 8, o qual informa que “Exemplos de implementações incluem controle de versão de destinos de *backup* por **meio de sistemas ou serviços *online,* na nuvem ou fora do site local**. ” <grifo nosso>. Também contraria o que estabelece a norma ABNT NBR ISO/IEC 17799, que trata da Tecnologia da informação

— Técnicas de segurança — Código de prática para a gestão da segurança da informação, em seu item 10.5.1, letra d.

VIII. A Sutin reconhece não realizar teste da recuperação do *backup*, conforme previsto na medida 11.5 do Relatório CIS.

À luz dos achados de auditoria, sugere-se:

I. À Sutin, fazer tratativas junto à Comissão Permanente de Avaliação de Documentos (CPAD) e à Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS) e criar iniciativa como o objetivo de definir a temporalidade das informações dos arquivos sob sua guarda, em conjunto com as áreas gestoras responsáveis pelas informações. Para esta iniciativa, observar as medidas 3.5 e 3.8 do Controle 03 Proteção de dados do Relatório Cis 8.

II. À Sutin para definir, normatizar e institucionalizar um processo de *backup*. Sugere-se que a normatização se dê por meio de manual de procedimentos (MAP), que são documentos de caráter orientativo e operacional.

III. À Sutin para promover o armazenamento, guarda e manutenção dos *logs* de processamento dos *backups* realizados e dos e-mails disparados. Cuidar para que a norma de *backup* inclua estes procedimentos.

IV. À Sutin para definir e implementar procedimentos de testes periódicos de recuperação de arquivos, de forma amostral, para atendimento ao que dispõe a medida 11.5 Testar os dados de recuperação, do Relatório Cis 8.

V. À Sutin para reavaliar a questão do local da guarda dos *backups*, em observância ao que dispõe a medida 11.4 Estabelecer e manter uma instância isolada de dados de recuperação, do Relatório Cis 8 e a norma ABNT NBR ISO/IEC 17799, item 10.5.1, letra d).

5.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

Encontra-se em fase de execução como projeto dentro da GEASI a produção de uma norma de backup e arquivamento que tem como objetivo estabelecer um processo que permita a SUTIN

e as demais áreas da Companhia a definição de temporalidade dos dados, assim como diferenciar, de forma institucionalizada, os prazos de arquivamento dos prazos de backup, assim como a formalização dos processos já executados dentro da Companhia.

No que tange a guarda de dados em espaço distinto ao do ambiente de computação, já foi alocado no planejamento de aquisições do ano corrente (2024) o orçamento necessário para aquisição de fitas para backup, o que permitirá utilizar um cofre, atualmente alocado no CDRH, como espaço para armazenamento das fitas provenientes deste serviço.

Quanto ao processo de testes de recuperação de dados, com a aquisição dos novos equipamentos de backup -- em processo de instalação -- deve-se tornar possível realizar a automação e padronização do processo de recuperação de dados por parte da equipe de backup. As outras medidas sugeridas serão implementadas junto a atualização da solução.

6 Análise do Risco 4 - Baixa maturidade dos processos envolvendo a disponibilidade dos serviços de TI, pois estes não estão formalmente definidos, instituídos, normatizados e documentados

6.1 Apresentação do Risco

Este risco pode gerar impacto no processo de Disponibilidade de Serviços de TI, comprometendo seu objetivo específico “Definir, documentar, instituir e normatizar os processos envolvendo a disponibilidade dos serviços de TI”.

A ausência de processos definidos e institucionalizados para a prestação dos serviços de TI pode causar atrasos na recuperação em caso de falhas e desastres ou, até mesmo, inviabilizá-la. Além disso, a falta da documentação dos processos faz com que todo o conhecimento de sua execução fique na cabeça dos técnicos, gerando dependência a estes, fragilizando desnecessariamente a prestação do serviço.

Com esta análise, pretende-se responder à seguinte questão de auditoria:

> “Como está a situação atual da Sutin em relação à definição, instituição e normatização dos processos de gestão de TI identificados na NOC 60.214? E qual a aderência dos processos definidos nessa Norma aos processos existentes na Cadeia de Valor da Conab, para a área de TI? ”

6.2. Análise do Risco

Os processos que envolvem a TI estão definidos na Cadeia de Valor da Conab, aprovada pelo Conselho de Administração por meio da Resolução Consad nº 021, de 16/12/2021.

Na ocasião, utilizou-se como suporte para definição dos processos de Gestão de TI, na referida Cadeia de Valor, a Biblioteca ITIL (*Information Technology Infrastructure Library*), versão 4.

No quadro abaixo, extraiu-se, da Cadeia de Valor, os processos relativos à gestão de serviços de TI, que correspondem ao processo de nível 1 “Gerir o suporte a serviços de TI” e seus respectivos processos de nível 2, a saber:

Quadro 12 – Cadeia de Valor – Gestão de suporte de serviços TI

Macroprocesso	Processo Nível 1	Processo Nível 2	Descrição	Responsável
Gestão de Tecnologia da Informação	Gerir o suporte a serviços de TI	Realizar a gestão de incidentes e requisições	Gerir a prestação de serviços de suporte técnico aos usuários, via aplicação SIGEDE	SUTIN
		Realizar a gestão de ativos, mudança e configuração	Gerir os ativos da infraestrutura de TIC, promovendo a execução dos procedimentos requeridos em caso de mudança e manter o controle efetivo de configuração e mudanças desses ativos (sistemas, aplicativos, objetos e serviços)	
		Realizar a gestão da disponibilidade	Executar os procedimentos necessários para garantir a disponibilidade dos serviços de TI nos níveis acordados, envolvendo a administração e o monitoramento do ambiente e infraestrutura e a implementação de melhorias	
		Realizar a gestão da continuidade	Garantir a disponibilidade e o desempenho dos serviços de TI em níveis suficientes em caso de desastres (ataques cibernéticos, desastres naturais etc), com a elaboração e execução de testes dos planos de contingências	
		Gerir o catálogo de serviços de TI	Realizar a manutenção do inventário de serviços de TIC, a gestão do Portfólio de TI e a celebração de acordo de níveis de serviços	
		Realizar a gestão da segurança da informação	Proteger as informações necessárias à Companhia, identificando e gerenciando os riscos para a confidencialidade, integridade e disponibilidade de informações	
		Realizar a gestão do conhecimento	Manter e melhorar o uso eficaz e eficiente da informação e do conhecimento requeridos para o planejamento, execução e entrega dos serviços oferecidos pela Sutin	

Fonte: Cadeia de Valor da Conab

A NORMA DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO (TI) (NOC 60.214) foi aprovada pela Resolução Diretoria Executiva N.º 007, de 06/09/2018, e tem por finalidade estabelecida em seu Capítulo I, item 3, “Estabelecer diretrizes e procedimentos relacionados

com a Gestão de Serviços de Tecnologia da Informação no âmbito da Companhia Nacional de Abastecimento (Conab)".

Em seu item 4, do mesmo capítulo, a NOC 60.214 define seu objetivo:

a. regulamentar os processos relacionados com a Gestão de Serviços de Tecnologia da Informação (TI), como Oficialização de Gestores de Sistemas de Informação, Gerenciamento de Incidentes e Requisições, Gerenciamento do Catálogo de Serviços, Gerenciamento da Configuração de Ativos de Serviço e Gerenciamento de Mudanças;
b. incorporar boas práticas em infraestrutura, operação e manutenção de serviços de TI com vistas a promover a efetiva implantação da governança de TI na Conab.

Vale destacar que a NOC 60.214 cita como suas fontes normativas (item 10, capítulo I) a norma ISO/IEC 20.000 e a Biblioteca ITIL (*Information Technology Infrastructure Library*), versão 3[31].

6.2.1 Comparativo Cadeia de Valor x NOC 60.214

Inicialmente, deve-se ressaltar que a elaboração da NOC 60.214 e sua inserção formal no arcabouço normativo da Companhia se deu em 06/09/2018, por meio da sua aprovação pelo Consad. Tal iniciativa demonstra a preocupação da Sutin com a definição e institucionalização de seus processos internos. Destaca-se, também, que a norma está bem amparada em termos conceituais, utilizando como fontes normativas a norma ISO/IEC 20.000 e a Biblioteca ITIL (*Information Technology Infrastructure Library*), o que também é um fator positivo.

Quadro 13 – Comparativo Cadeia de Valor x NOC 60.214

Cadeia de Valor		NOC 60.214	
Processo Nível 2	**Descrição**	**Local**	**Descrição**
Realizar a gestão de incidentes e requisições	Gerir a prestação de serviços de suporte técnico aos usuários, via aplicação SIGEDE	CAPÍTULO V GERENCIAMENTO DE INCIDENTES E REQUISIÇÕES	O objetivo principal do processo é restaurar os serviços disponíveis, quando ocorrer um incidente, e tratar as requisições de serviço de tal forma que tanto o incidente quanto as requisições respeitem o Nível Mínimo de Serviço (NMS) com base no histórico dos atendimentos realizados.

31 A NOC 60.214 foi publicada em 06/09/2018 e a versão 4 desta Biblioteca só veio a ser lançada em 2019.

Realizar a gestão de ativos, mudança e configuração	Gerir os ativos da infraestrutura de TIC, promovendo a execução dos procedimentos requeridos em caso de mudança e manter o controle efetivo de configuração e mudanças desses ativos (sistemas, aplicativos, objetos e serviços)	CAPÍTULO VI - GERENCIAMENTO DE CONFIGURAÇÃO E DE ATIVOS DE SERVIÇO	Estabelecer e manter a integridade de todos os produtos de trabalho de um processo ou operação do serviço e disponibilizá-los a todos os envolvidos
		CAPÍTULO VII - GERENCIAMENTO DE MUDANÇAS	Assegurar que todas as mudanças que afetam os serviços sejam avaliadas, aprovadas, implementadas e revisadas de maneira controlada.
Realizar a gestão da disponibilidade	Executar os procedimentos necessários para garantir a disponibilidade dos serviços de TI nos níveis acordados, envolvendo a administração e o monitoramento do ambiente e infraestrutura e a implementação de melhorias		
Realizar a gestão da continuidade	Garantir a disponibilidade e o desempenho dos serviços de TI em níveis suficientes em caso de desastres (ataques cibernéticos, desastres naturais etc), com a elaboração e execução de testes dos planos de contingências		
Gerir o catálogo de serviços de TI	Realizar a manutenção do inventário de serviços de TIC, a gestão do Portfólio de TI e a celebração de acordo de níveis de serviços	CAPÍTULO IV - GERENCIAMENTO DO CATÁLOGO DE SERVIÇOS	Fornecer e manter uma única fonte de informações consistente sobre todos os serviços operacionais, prestados pela Sutin, e aqueles que estão sendo preparados para entrar em produção garantindo que estejam disponíveis somente para aqueles que estão autorizados a acessá-los.
Realizar a gestão da segurança da informação	Proteger as informações necessárias à Companhia, identificando e gerenciando os riscos para a confidencialidade, integridade e disponibilidade de informações		
Realizar a gestão do conhecimento	Manter e melhorar o uso eficaz e eficiente da informação e do conhecimento requeridos para o planejamento, execução e entrega dos serviços oferecidos pela Sutin		

Fonte: Audin

Do ponto de vista da Norma NOC 60.214, há tratamento para 3 dos 7 processos definidos na Cadeia de Valor da Conab, a saber: a) realizar a gestão de incidentes e requisições; b) realizar a gestão de ativos, mudança e configuração; e c) gerir o catálogo de Serviços de TI.

A propósito dos processos da Cadeia que não estão previstos na NOC 60.214, cabem as seguintes considerações:

a. Os processos "Realizar a gestão da disponibilidade" e "Realizar a gestão da continuidade" são o objeto de estudo da presente auditoria. Espera-se que esta venha a gerar subsídios para a complementação destas lacunas na norma NOC 60.214, quando de sua revisão.
b. No que concerne ao processo "Realizar a gestão da segurança da informação", a NORMA DE RECURSOS COMPUTACIONAIS – 60.213, aprovada pela Resolução Direx nº 024 de 23/11/2020, trata dessa matéria do ponto de vista operacional, isto é, da utilização dos serviços. Do ponto de vista de diretrizes de segurança da informação, convém mencionar a Política de Segurança da Informação – NOC 10.010. Dessa forma, o processo "Realizar a gestão da segurança da informação" é tratado de forma independente e fora da norma de gestão de serviços e TI (NOC 60.214), por meio de outras normas aprovadas posteriormente à aprovação da NOC 60.214[32].
c. O processo "Realizar a gestão do conhecimento" permanece como uma lacuna na NOC 60.214.

6.2.2 Implementação da NOC 60.214

Para cada processo definido nos capítulos IV a VII (GERENCIAMENTO DE INCIDENTES E REQUISIÇÕES, GERENCIAMENTO DE CONFIGURAÇÃO E DE ATIVOS DE SERVIÇO, GERENCIAMENTO DE MUDANÇAS e GERENCIAMENTO DO CATÁLOGO DE SERVIÇOS), a Norma NOC 60.214 estabelece as diretrizes gerais de funcionamento do processo e, ao final de cada capítulo citado, a norma traz a recomendação de elaboração de normas específicas (NICs) para detalhamento de procedimentos envolvidos no referido processo.

32 A NOC 60.214 foi aprovada em 06/09/2018, a NOC 10.010 em 17/12/2019 e a NOC 60.213 em 23/11/2020

Atualmente, de acordo com a NORMA DE GESTÃO NORMATIVA (NOC 60.304) as NIC passaram a chamar-se Manual de Procedimentos (MAP)[33].

Em que pese estar bem ancorada conceitualmente e bem estruturada, a NOC 60.304, a norma ainda não pode ser considerada completamente institucionalizada. Ocorre que, à exceção da NIC – GERENCIAMENTO DE MUDANÇAS – 60.214-01, nenhuma das demais NICs previstas na NOC 60.214 foi elaborada, ficando a implementação integral da NOC 60.214 prejudicada, no que concerne aos processos citados.

6.3. Conclusão

Com base na exposição anterior, temos a seguinte síntese dos achados:

I. A elaboração e institucionalização da NORMA DE GESTÃO DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO (TI) (NOC 60.214) é fator positivo para a gestão de TI, na Conab. A norma está bem amparada em termos conceituais, utilizando como fontes normativas a norma ISO/IEC 20.000 e a Biblioteca ITIL (*Information Technology Infrastructure Library*).

II. A Norma NOC 60.214 dá tratamento a 3 dos 7 processos definidos na cadeia de valor: Realizar a gestão de incidentes e requisições, realizar a gestão de ativos, mudança e configuração e gerir o catálogo de Serviços de TI.

III. Para os processos da Cadeia de Valor não contemplados pela norma, temos que:

Processos “Realizar a gestão da disponibilidade” e” Realizar a gestão da continuidade”: são o objeto de estudo da presente auditoria, que pode dar subsídios para a atualização da norma.

Processo ““Realizar a gestão da segurança da informação”: há normas específicas que tratam da matéria (NORMA DE RECURSOS COMPUTACIONAIS – 60.213 e a Política de Segurança da Informação – NOC 10.010).

Processo “Realizar a gestão do conhecimento” permanece como uma lacuna na NOC 60.214.

33 Manual de Procedimentos (MAP): É um documento de caráter orientativo e operacional, que facilita a interpretação das NOCs. O MAP deve descrever as instruções, fluxos de processos e orientações detalhadas dos procedimentos, atividades e tarefas dos macroprocessos constantes nos normativos internos. (MAP – GESTÃO NORMATIVA – 60.304-01, capítulo I, item I)

IV. Para os processos definidos na NOC 60.214, esta estabelece as diretrizes gerais e indica que o detalhamento deverá ser dado por meio de NIC específica. Ocorre que, à exceção da NIC – GERENCIAMENTO DE MUDANÇAS – 60.214-01, nenhuma das NIC foi elaborada, ficando a implementação integral da NOC 60.214 prejudicada.

À luz dos achados de auditoria sumarizados acima, sugere-se:

I. Revisão da NOC 60.214 de modo a contemplar as lacunas apontadas no Quadro 02: a) Inclusão dos processos "Realizar a gestão da disponibilidade" e "Realizar a gestão da continuidade", utilizando como subsídios os apontamentos desta auditoria; b) incluir o processo "Realizar a gestão do conhecimento", observando a descrição deste prevista na Cadeia de Valor: "Manter e melhorar o uso eficaz e eficiente da informação e do conhecimento requeridos para o planejamento, execução e entrega dos serviços oferecidos pela Sutin"; c) quanto ao processo "Realizar a gestão da segurança da informação", avaliar a conveniência e oportunidade de incluí-lo na NOC 60.214, por meio de diretrizes gerais, fazendo referência às normas demais pertinentes (NORMA DE RECURSOS COMPUTACIONAIS – 60.213 e a Política de Segurança da Informação – NOC 10.010). Além disso, realizar a revisão e atualização destas duas normas, caso necessário.
II. Elaboração de Manual de Procedimentos (MAP) específico previsto na NOC 60.214, com o detalhamento dos procedimentos referentes aos processos GERENCIAMENTO DE INCIDENTES E REQUISIÇÕES, GERENCIAMENTO DE CONFIGURAÇÃO E DE ATIVOS DE SERVIÇO, e GERENCIAMENTO DO CATÁLOGO DE SERVIÇOS
III. Para a NIC – GERENCIAMENTO DE MUDANÇAS – 60.214-01, já elaborada, promover sua revisão e atualização, caso seja necessária, inclusive transformando-a em MAP.

6.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

Como parte da gestão de serviços, estamos iniciando a implementação do processo de gestão de conhecimento e a atualização do processo de gestão de configuração e mudanças, com o objetivo de publicar uma MAP da NOC 60.214 ainda esse ano. Quanto aos processos de gestão

de disponibilidade e gestão de continuidade, iremos adicionar aos planos de trabalho da SUTIN a previsão de implementação destes processos para período 2/2024 e 1/2025. É importante frisar que o modelo adotado na SUTIN para implementação das disciplinas do ITIL consiste em primeiro definir uma estratégia de implementação, normalmente por meio de um grupo de trabalho formado por empregados de todas as gerências, e apenas após uma implementação piloto e adesão ao processo como parte da cultura da SUTIN, produzir as MAPs e alterações na NOC

7 Análise do Risco 5 - Monitoramento não adequado da disponibilidade de sistemas e serviços

7.1. Apresentação do Risco

Este risco pode gerar impacto no processo de Disponibilidade de Serviços de TI, comprometendo seu objetivo específico "Acompanhar e monitorar o fornecimento dos serviços de TI para que estes ocorram em níveis adequados e acordados, executando os ajustes que se fizerem necessários".

O monitoramento do ambiente pode antecipar possíveis falhas em ativos (equipamentos, rede, *softwares*, aplicações etc.) ou permite agir de forma proativa para minimizar o impacto destas, uma vez que esta identificação é feita prematuramente, antes mesmo que o usuário venha a reportar a falha do serviço.

O processo de monitoramento envolve a utilização de ferramentas adequadas, de um processo definido e de pessoas treinadas para executá-lo.

A análise deste risco pretende responder à seguinte questão de auditoria:

> "Como tem sido realizado o processo de monitoramento da disponibilidade de sistemas e serviços de TI na Conab? "

7.2. Análise do Risco

A análise do risco deverá prover subsídios para responder à questão de auditoria citada. Inicialmente, vale a pena ressaltar a importância e vantagens de realizar-se o monitoramento da disponibilidade de serviços de TI, pelas razões que se seguem:

a) **Garantir a disponibilidade e confiabilidade:** o monitoramento ajuda a garantir que os serviços de TI entejam sempre disponíveis e funcionando de forma confiável, de modo a promover a produtividade e a satisfação dos usuários.
b) **Identificar problemas precocemente:** O monitoramento permite detectar problemas e anomalias nos serviços de TI antes que eles causem interrupções graves. Por exemplo, a degradação de um serviço, via parâmetros como tempo de resposta, pode indicar que o provavelmente o serviço irá ficar indisponível em breve. O

monitoramento pode permitir uma atuação proativa, verificando a causa da degradação e a adoção de medidas corretivas, antes que o problema afete os usuários.

c) **Otimização de Recursos:** Ao monitorar o desempenho dos serviços de TI, podem-se identificar áreas nas quais os recursos estão sendo subutilizados ou superutilizados, possibilitando a otimização do uso de recursos de *hardware* e *software.*

d) **Segurança da Informação:** O monitoramento também desempenha um papel fundamental na segurança da informação. Ele ajuda a identificar atividades suspeitas, como tentativas de invasão ou acessos não autorizados, para que medidas de segurança adequadas possam ser tomadas.

e) **Melhoria Contínua:** O monitoramento fornece dados valiosos que podem ser usados para análise e melhoria contínua dos serviços de TI. Com base nos dados coletados, pode-se fazer ajustes, atualizações e otimizações visando à referida melhoria.

Segundo a prática da ITL v4, "Monitoramento e gerenciamento de evento", temos que:

> O propósito da prática de monitoramento e gerenciamento de evento é observar sistematicamente os componentes de serviços e serviços e registrar e relatar mudanças selecionadas de estado identificadas como eventos. Essa prática identifica e prioriza a infraestrutura, os serviços, os processos de negócios e os eventos de segurança das informações e estabelece a resposta adequada a esses eventos, incluindo a resposta a *condições que podem levar a possíveis falhas ou incidentes.*

Segundo a Sutin (SA n° 4), o processo de monitoramento da disponibilidade dos serviços na Conab é feito de forma parcial, cobrindo apenas a camada de infraestrutura. Sistemas e serviços não são monitorados para a aferição da disponibilidade.

Em entrevista, o gestor da Geasi ratificou esta assertiva. No que concerne ao monitoramento da infraestrutura, informou que é realizada por meio da ferramenta denominada Zabbix.

O Zabbix é uma solução de monitoramento de código aberto projetada para monitorar o desempenho e a disponibilidade de serviços de rede, servidores, dispositivos e aplicativos em ambientes de TI. Ela permite coletar, processar, armazenar e analisar dados de desempenho em tempo real de diversos ativos de TI, como servidores, roteadores, *switches*, aplicativos etc. e fornece informações críticas sobre o estado e o desempenho desses ativos para ajudar as equipes de TI a detectar problemas, tomar medidas corretivas e otimizar a infraestrutura de TI.

Segundo o gestor da Geasi, quando da criação de uma máquina virtual[34], o *software* Zabbix é instalado, permitindo o monitoramento de atributos do servidor como uso de disco, memória, processador, uso da rede, dentre outros. Desta forma, todos os servidores da rede da Conab estão sendo monitorados pelo Zabbix.

Quanto ao monitoramento de aplicações, segundo o gestor da Geasi, a Sutin não a realiza em regra, mas vem realizando o monitoramento do Sistema de Fiscalização (Sifisc) por meio do *software* Zabbix; tratando-se, todavia, de uma experiência isolada e limitada, capaz de verificar apenas se a aplicação está *online* ou não.

No entendimento do gestor, a adoção plena do monitoramento de aplicações deverá contemplar aspectos para além da simples constatação se a aplicação está *online* ou não, envolvendo outras funcionalidades como, por exemplo, a verificação se a aplicação começou a entrar em processo de degradação do seu tempo de resposta. Além do prejuízo da *performance* em si, essa degradação pode representar sintomas de problemas sistêmicos tais como comunicação com o banco de dados ou de conexão entre componentes da aplicação.

Conforme já comentado, um processo de monitoramento deveria gerar informações para permitir que a equipe de TI pudesse agir de forma proativa, corrigindo o problema antes que ele viesse a gerar interrupções no fornecimento do serviço.

A solução, segundo o gestor, é que a Sutin desenhe e implemente uma iniciativa para a prospecção de ferramentas de monitoramento de aplicações mais robustas, com vista à avaliação e à seleção de uma ferramenta de monitoramento adequada às necessidades e requisitos da Sutin.

A seguir, apresenta-se um conjunto de funcionalidades desejáveis para uma ferramenta de monitoramento de aplicações. Importante ressaltar que estas funcionalidades devem ser vistas no contexto das necessidades da Sutin:

- **Coleta de Dados em Tempo Real**: A ferramenta deve ser capaz de coletar dados de desempenho e métricas em tempo real dos componentes da aplicação, como

34 Um servidor de dados físico pode ser dividido em diversas máquinas virtuais. Trata-se de uma estratégia útil para otimizar o uso dos recursos

servidores, bancos de dados, serviços da *web*, entre outros, para detectar problemas ou anomalias.

- **Alertas e Notificações:** Deve oferecer recursos de alerta configuráveis para notificar as equipes de operações ou desenvolvimento quando ocorrem problemas ou anomalias detectadas no monitoramento ou, ainda, quando métricas ultrapassam limites predefinidos. As notificações podem ser feitas por meio de e-mails, mensagens instantâneas ou outras ferramentas de alerta.
- **Visualização de Dados:** Deve permitir a criação de painéis personalizados e gráficos para visualizar métricas de desempenho de forma eficaz. A visualização clara ajuda na identificação rápida de problemas.
- **Armazenamento de Dados de Longo Prazo:** Deve ser capaz de armazenar dados históricos de desempenho para análises de tendências e geração de relatórios. Além disso, manter registros detalhados das mudanças e atividades de monitoramento para fins de auditoria e conformidade.
- **Rastreamento de Transações:** Deve fornecer visibilidade detalhada sobre como as transações estão funcionando por meio da aplicação, permitindo a identificação de gargalos e lentidões.
- **Monitoramento de Múltiplas Camadas:** Deve ser capaz de monitorar todos os aspectos da aplicação, incluindo infraestrutura, redes, servidores, bancos de dados e código da aplicação.
- **Análise e Correlação de Dados:** Deve ser capaz de analisar e correlacionar dados de diferentes fontes para ajudar a identificar as causas raiz de problemas de desempenho.
- **Integração com Outras Ferramentas:** Deve poder integrar-se facilmente com outras ferramentas de TI adotadas na Sutin.
- **Escalabilidade:** Deve ser escalável para acomodar o crescimento da infraestrutura e a adição de novas aplicações, sem perda de desempenho.
- **Segurança:** Deve garantir a segurança dos dados coletados e das comunicações, incluindo recursos de autenticação e autorização.
- **Customização e Extensibilidade:** Deve permitir a personalização e extensão para atender às necessidades específicas da sua organização.

- **Suporte à Análise de *Logs*:** A capacidade de coletar e analisar *logs* de aplicação é importante para diagnósticos avançados.
- **Modelagem de Dependências:** Pode identificar e mapear as dependências entre componentes da aplicação para facilitar a detecção de impactos, quando ocorrem problemas.

No seu contexto atual, por não dispor de uma solução para monitoramento de sistemas e serviços, a Sutin toma conhecimento de incidentes relativos à disponibilidade de sistemas e serviços de forma reativa, via o Sistema de Gestão de Demandas (SIGEDE), que é o canal oficial pelo qual os usuários comunicam os referidos incidentes.

A questão do monitoramento da disponibilidade de sistemas e serviços tangencia outra questão, associada à definição de acordos de níveis de serviços (SLA), discutidos na análise do risco "6. Inexistência de um processo definido, implantado e testado para recuperação em caso de desastres". Como não há definição, na Sutin, de Acordos de Níveis de Serviços (*Serviçe Level Agreement* – SLA, em inglês), ou seja, não estão definidos junto às áreas gestoras dos serviços, as metas de disponibilidade e suporte para o referido serviço/aplicação, não há como mensurar de forma objetiva se a disponibilidade dos sistemas e serviços está ocorrendo em níveis satisfatórios.

Segundo a prática "**Gerenciamento de nível de serviço" da ITIL v4**, temos que**:**

> *O propósito da prática de gerenciamento de nível de serviço é definir metas claras de negócios para níveis de serviço e garantir que a entrega de serviços seja avaliada, monitorada e gerenciada adequadamente em relação a essas metas.*

A NOC de Gestão de Serviços de TI (NOC 60.641) traz a previsão de cumprimento de Nível Mínimo de Serviço (NMS), quando do atendimento de requisições de Serviço, via Sigede. O conceito de NMS estabelecido na norma é de "É um valor de tempo geralmente em horas, estabelecido pela área de TI para o atendimento de uma demanda apresentada". A rigor, o NMS reflete apenas a capacidade de atendimento da Sutin, não a disponibilidade do serviço em si, embora esta seja afetada pelo NMS.

Além disso, a Sutin não dispõe de indicadores definidos e implementados para permitir o acompanhamento da disponibilidade dos serviços de TI.

7.3. Conclusão

Com base na exposição anterior, temos a seguinte síntese dos achados:

I. A Sutin realiza o monitoramento da infraestrutura via *software* Zabbix. A Sutin não realiza o monitoramento de disponibilidade de sistemas, em regra. Há uma exceção, a Sutin vem utilizando o zabbix para monitoramento do Sistema de Fiscalização (Sifisc), mas além de ser uma experiência isolada, este monitoramento é capaz de verificar apenas se a aplicação está *online* ou não.

II. A Sutin não dispõe de uma ferramenta para monitoramento de sistemas e serviços de TI com funcionalidades para além de saber se a aplicação está ativa ou não.

III. Não há indicadores definidos / implementados para permitir o acompanhamento da disponibilidade dos serviços de TI.

IV. Não há definição de Acordos de Níveis de Serviços (*Serviçe Level Agreement* – SLA, em inglês).

À luz dos achados de auditoria sumarizados acima, sugere-se:

i. À Sutin para definir e implementar iniciativa que envolva: a) prospecção de ferramentas de monitoramento mais robustas, com funcionalidades para além da que vem sendo adotada no caso do sistema Sifisc; b) seleção de uma ferramenta de monitoramento para avaliação; e c) definição de uma estratégia para a implantação da ferramenta selecionada na Sutin.

ii. Definir iniciativa e plano de ação para a definição de: a) Acordos de Níveis de Serviços (*Serviçe Level Agreement* – SLA, em inglês) para os serviços de TI disponibilizados e prestados pela Sutin; b) definição e implementação de indicadores para o acompanhamento da disponibilidade de serviços de TI.

7.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

A GEASI está planejando a prospecção de solução de monitoramento de aplicações como um dos projetos do segundo semestre de 2024, de forma a implementar as sugestões da auditoria.

Tal solução deve estar focada no monitoramento de aplicações e rastreabilidade (tracing), permitindo não apenas identificar indisponibilidade como também erros e lentidão. A definição de indicadores e de prazos de atendimento deve ser realizada em conjunto com as gerências de desenvolvimento e manutenção de sistemas, respectivamente, GESIN e GEMAN.

8 Análise do Risco 6 - Inexistência de um processo definido, implantado e testado para recuperação em caso de desastres

8.1 Apresentação do Risco

Este risco pode gerar impacto no processo de Disponibilidade de Serviços de TI, comprometendo seu objetivo específico “Realizar ações para garantir a continuidade do fornecimento dos serviços de TI em caso de desastres ou falhas”.

As possíveis consequências da materialização do risco são: atrasos ou recuperação incompleta dos ativos de TI, indisponibilidade dos serviços de TI, paralização de processos chave da Companhia por tempo acima do desejável ou aceitável.

Com esta análise, pretende-se responder à seguinte questão de auditoria:

> “Há processo formal definido e implantado para recuperação de desastres? Se não, qual a situação atual da implementação dos processos envolvidos, considerando em especial aqueles definidos no PCN e nas Normas Complementares do Governo Federal”.

8.2 Análise do Risco

A análise deverá prover subsídios para responder à questão de auditoria citada. Para tanto, discorrerá sobre os aspectos relativos a criação de uma a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, atendimento de exigências do Plano de Continuidade de Negócios (PCN) da Companhia e, por fim, fará uma avaliação dos resultados obtidos pela Conab no diagnóstico realizado pelo TCU para a segurança cibernética na Conab.

8.2.1. Criação da ETIR

Segundo a Norma Complementar 05/IN01/DSIC/GSIPR78, a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR - é o grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

A mesma Instrução Normativa define Tratamento de Incidentes de Segurança em Redes Computacionais como o serviço que consiste em receber, filtrar, classificar e responder às

solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e, também, a identificação de tendências.

O PDTIC 2021-2024 já previa a criação de uma Equipe para tratamento e Resposta a incidentes em Redes computacionais (ETIR) em seu item 10. PLANO DE METAS E AÇÕES, via ação AC28:

> AC28 Desenvolver projeto para elaboração de norma e formalização de Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR.

A Norma Complementar 05/IN01/DSIC/GSIPR78 disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, nos órgãos e entidades da Administração Pública Federal.

A ETIR-Conab foi implementada por meio de ato de superintendência nº 8, de 20/12/2022, constante no processo 21200.005599/2022-13.

O Ato de criação da ETIR-Conab contemplou os itens previstos na Norma Complementar nº 05/IN01/DSIC/GSIPR78. Segundo o ato constitutivo da Equipe:

> *A ETIR-Conab tem como missão promover a segurança em tecnologia da informação e comunicação na Conab por meio de* ***processos, ferramentas e estratégias de prevenção, tratamento e resposta à incidentes cibernéticos,*** *observando as boas práticas, as normas e os procedimentos estabelecidos pela Companhia, pelo governo federal e por demais instituições e profissionais relevantes do mercado <grifo nosso>.*

O conteúdo do Ato de criação da ETIR é bastante específico e detalhado, versando sobre itens como objetivos da ETIR, forma de atuação, serviços prestados (serviços preventivos e reativos), estrutura organizacional, canais de comunicação, etc.

O Ato prevê também a criação de uma série indicadores, que foram sintetizados no quadro a seguir:

Quadro 14 – Indicadores previstos no Ato de criação da ETIR

Tipo de Serviço/Natureza	Indicador
Serviços Preventivos	
Varreduras periódicas de vulnerabilidade	Percentual da quantidade de vulnerabilidades corrigidas em relação à quantidade de vulnerabilidades encontradas por mês.
Serviços Reativos	
Tratamento de incidente cibernético	Quantidade de incidentes registrados, resolvidos e não resolvidos;
	Tempo médio de duração de um incidente por mês.
Notificação de incidente cibernético	Quantidade de incidentes cibernéticos relevantes comunicados em relação ao total de incidentes relevantes tratados por mês;

	Tempo médio de notificação de um incidente cibernético após seu registro por mês.
Processamento de alertas e recomendações	Quantidade de alertas processados em relação aos recebidos por mês;
	Quantidade de recomendações processadas em relação as recebidas por mês.
Serviços de gestão de qualidade	
Análise de Maturidade em Segurança de Tecnologia da Informação (controles CIS)	Índice anual de maturidade, conforme definido pela ferramenta CIS-CSAT v8;
	Taxa de evolução da maturidade por ano.

Fonte: Ato de Superintendência nº 8, de 20/12/2022.

A previsão de uma quantidade e variedade de indicadores propostos, associados aos diversos serviços a serem prestados, é um ponto positivo para a implementação dos serviços previstos pela ETIR-Conab, pois permitem acompanhar os serviços prestados, nos seus diversos momentos, as ações preventivas, as notificações dos incidentes e o tratamento dado a estes, além dos indicadores relativos à maturidade do processo.

Cabe lembrar que não há acordos de níveis de serviço (SLA) definido para a prestação dos serviços de TI, de modo a indicar a disponibilidade acordada destes serviços para os usuários, conforme resposta à questão 3 da Solicitação de Auditoria 04: "Não há acordos de níveis de serviços para a disponibilidade de sistemas e serviços. Porém, existem acordos de níveis mínimos de serviços definidos para o atendimento no escopo do Sistema de Gestão de Demandas (SIGEDE) ".

O indicador Nível Mínimo de Serviço (NMS) definido para o SIGEDE refletem o tempo para o atendimento da demanda do usuário, após o incidente, podendo afetar a disponibilidade do serviço (pois, quanto mais tempo para resolver o chamado relativo a um incidente, mais tempo de indisponibilidade), mas não a definir. O SLA, por sua vez, possui um sentido mais amplo e proposta mais ambiciosa, ao formalizar o compromisso assumido pela área de TI com a disponibilidade do Serviço de TI, indicando que esta área terá de estruturar-se para tanto.

Assim, ressentiu-se de indicadores que demonstrem: a) o tempo médio gasto para a recuperação do ambiente operacional e a disponibilização dos serviços de TI, após a ocorrência do incidente. Este indicador poderia ser uma melhoria do indicador "Tempo médio de duração de um incidente por mês", já previsto (*vide* quadro 14); e b) a definição de acordos de níveis de serviços (SLA) que orientariam se há disponibilidade dos serviços de TI, e seu cumprimento nos casos de falhas na prestação do serviço por incidentes.

A criação da ETIR, na Conab, nos termos propostos pelo seu ato de criação é uma iniciativa salutar e oportuna. Sua implementação integral significa um grande desafio para a Sutin, seja pela extensão das mudanças, seja pela quantidade de esforços humanos e recursos técnicos requeridos. Observe-se que o item "Missão" da Equipe ETIR cita que sua atuação deverá ser por meio de **processos, ferramentas e estratégias de prevenção, tratamento e resposta a incidentes cibernéticos**. O item "objetivos" também elenca uma série de medidas e atividades que envolvem mudança de processos de trabalho.

Observando o escopo, abrangência do conteúdo do Ato de criação da ETIR-Conab e as implicações das ações ali propostas já citadas, o entendimento desta auditoria é que este conteúdo deveria ter suas diretrizes inseridas na Norma de gestão de Serviços (NOC 60.214), quanto ao Processo de nível 2 "Realizar a Gestão da continuidade", previsto na Cadeia de Valor, vide análise do Risco 4 – "Baixa maturidade dos processos envolvendo a disponibilidade dos serviços de TI, pois estes não estão formalmente definidos, instituídos, normatizados e documentados" no item 6 deste relatório. Além disso, deveria ter seus procedimentos detalhados em uma MAP específica. Esta proposta encontra respaldo no PDTIC 2021-2024, que já previa a elaboração de norma para tratar a matéria, via ação AC28 "Desenvolver projeto para elaboração de norma e formalização de Equipe de Tratamento e Resposta a Incidentes Cibernéticos – ETIR" do seu Plano de ações e metas. Além disso, a inserção da criação da ETIR-Conab no arcabouço normativo da Companhia, via NOC 60.214, dará mais estabilidade à iniciativa.

Tendo em vista os desafios relacionados à efetiva implementação da ETIR-Conab, a Sutin foi questionada, por meio da Solicitação de Auditoria nº 7, sobre o estado de implementação da ETIR-Conab, quais a providências tomadas e o seu estágio de implementação, indicando as evidências das providências e implementações.

Não foram apresentadas evidências da efetiva implementação da ETIR-Conab pela Sutin. Em que pese a ausência de informações nesse sentido, deve-se levar em conta que a criação da ETIR-Conab é uma iniciativa relativamente recente, tendo sido criada há pouco mais de 8 meses (20/12/2022).

A propósito das evidências solicitadas quanto à Implementação da ETIR-Conab, a resposta à questão 10 da Solicitação de Auditoria n° 4, sobre casos de ataques cibernéticos ao portal corporativo, trouxe uma referência à atuação da Equipe ETIR:

> *As tentativas de ataques cibernéticos são constantes sendo a maioria do tipo phishing, ou seja, voltado para obtenção de credenciais de usuários por meio de mensagens fraudulentas contendo links maliciosos.* ***Quando há suspeita de vazamento de credenciais, a Equipe de Prevenção, Tratamento e Resposta à incidentes cibernéticos da Conab atua nas medidas corretivas, como por exemplo, no bloqueio dos links e na alteração da senha dos usuários supostamente afetados****. <grifo nosso>*

8.2.2. Atendimento ao Plano de Continuidade do Negócio (PCN)

A Resolução CGPAR Nº 11/2016 definiu que a Conab deveria possuir uma Gestão de Continuidade de Negócios. Com objetivo de dar cumprimento à citada resolução, a Diretoria Executiva da Conab aprovou o Plano de Continuidade do Negócio (PCN), em sua milésima quingentésima decima reunião ordinária.

O PCN é composto por quatro planos menores: o Plano de Administração de Crises (PAC), o Plano de Contingência (PC), o Plano de Recuperação de Desastres (PRD) e o Plano de Continuidade Operacional (PCO).

Durante o trabalho de Auditoria, a Sutin foi indagada sobre a existência de um Plano de Continuidade específico para os processos de TI, de forma integrada ao PCN, ou a dar suporte a este, e, também, sobre a existência do Time de Recuperação de Desastres (TRD-Sutin), previsto no Plano de Recuperação de Desastres (PRD), do PCN, e suas competências. Para ambos os casos, a Sutin informou não terem sido implementados ainda.

No entendimento desta auditoria, a Equipe de Tratamento e Resposta a incidentes em Redes computacionais (ETIR-Conab), uma vez implementada conforme seu ato de criação, pode vir a suprir as demandas do PCN, quanto ao Time de Recuperação de Desastres (TRD- Sutin), desde que implementados os eventuais ajustes que se fizerem necessários.

No que concerne ao plano de continuidade específico para os processos de TI, de forma integrada ao PCN, vale a pena analisar as respostas dadas pela Sutin às questões 8, 9 e 10 da Solicitação de Auditoria n° 4, que tratou do processo de recuperação em caso de falhas e/ou desastres:

> *A Sutin monitora a infraestrutura e acompanha o funcionamento dos sistemas e serviços de TI. Sempre que é detectado algum desastre, passa a atuar na sua recuperação. Normalmente, um dos gestores da Sutin percebe o problema ou é acionado por alguma área impactada por ele e passa a avaliar a natureza do incidente, buscando identificar a área regimentalmente responsável e acionar, se for o caso, o gerente responsável informando o*

> *Superintendente da área sobre o incidente. O gerente aciona a equipe técnica que realiza um diagnóstico inicial e avalia a extensão, o tipo e os prováveis impactos do incidente. Os analistas e técnicos com maior conhecimento são acionados e, então, é iniciado o processo de correção e/ou recuperação dos sistemas afetados. Uma avaliação da correlação de serviços e sistemas pode ser necessária e deverá ser feita a partir das informações documentadas no catálogo de aplicações da SUTIN (http://geasiwiki.conab.gov.br/wiki/index.php/Categoria:CatalogoAplicacoesSutin).*
>
> *Durante a atuação na recuperação, a equipe técnica envolvida vai informando aos gestores sobre fatos relevantes ou questões que envolvem alguma decisão estratégica, enquanto os gestores vão acompanhando e reportando para o público-alvo dos serviços afetados e para a alta gestão as orientações, previsões e demais informações necessárias.*

Por esta descrição, observa-se que a Sutin possui processo definido, entretanto, ressente-se da formalização, institucionalização e normatização deste[35]. Sobre o assunto, valem as observações feitas e as alterações propostas para a revisão da NOC 60.214, no item 6 deste relatório.

O Relatório **"**Acompanhamento de Controles Críticos de Segurança Cibernética das Organizações Públicas Federais", elaborado pelo Tribunal de Contas da União e encaminhado à Conab por meio do Processo SEI nº 21200.005504/2021-72, apresentou a avaliação de controles e medidas consideradas críticas no contexto da segurança cibernética na Companhia. Segundo este Relatório, a Sutin informa não possuir um processo formalmente aprovado e documentado de gestão de vulnerabilidades e de correção destas.

O item Diagnóstico TCU para segurança cibernética na Conab será apresentado a seguir, no qual discutir-se-á melhor seus achados.

Quanto à ocorrência de incidentes que envolvam acesso indevido ao ambiente de TI, no período entre 2019 e 2023, a Sutin informou que ocorreu apenas um incidente em 2019, que decorreu de falha nos controles relativos à atualização de versão de *software* e de configuração de *software*, que acabaram por gerar a vulnerabilidade. Como a ferramenta de detecção de invasão (IDS) estava desabilitada, outra falha de controle, a vulnerabilidade foi explorada. À

35 Na Estrutura COSO IC-IF 2013 (p. 108), o framework dispõe que políticas e procedimentos não formalizados (escritos) podem ser contornados mais facilmente, ter um custo elevado para a organização no caso de elevado turnover de profissionais, além de reduzir a responsabilidade pela prestação de contas.

luz desses dados e considerando o período analisado, trata-se de um número pequeno de incidentes.

Entretanto, para a gestão do processo, é importante que haja indicadores definidos e implementados para acompanhamento dos incidentes cibernéticos, em todas as suas fases, de forma objetiva e sistemática. A propósito do assunto, o Ato de criação da ETIR-Conab prevê a criação e implementação desses indicadores.

8.2.3 Diagnóstico TCU para segurança cibernética na Conab

Por fim, vale a pena lançar um olhar sobre os resultados apurados pelo Relatório **"**Acompanhamento de Controles Críticos de Segurança Cibernética das Organizações Públicas Federais", pela estreita relação com o risco analisado, pois falhas nos controles de segurança dos processos podem levar a maiores incidentes e comprometer a continuidade dos serviços de TI, inclusive.

Trata-se de pesquisa realizada pelo Tribunal de Contas da União (TCU), de forma *online*, no período de 11/10 a 5/11/2021, para avaliar a adoção, pelas Organizações Públicas Federais, de controles e medidas consideradas críticas no contexto da segurança cibernética. A Conab participou desta pesquisa e os seus resultados serão apresentados e discutidos a seguir.

A pesquisa do TCU avaliou as medidas básicas dos seguintes controles:

a) Inventário e controle de ativos corporativos
b) Inventário e controle de ativos de *softwares*
c) Gestão contínua de vulnerabilidades
d) Conscientização sobre segurança e treinamento de competências
e) Gestão de resposta a incidentes

Para a avaliação e classificação dos resultados, o TCU definiu um indicador denominado iSegCiber, calculado[36] a partir da avaliação dos respondentes (autodeclaratória) para as medidas previstas para os controles avaliados. O resultado do iSegCiber permite a classificação do nível da organização avaliada, a partir da definição das seguintes faixas de resultados:

36 A fórmula de cálculo do indicador é detalhada pelo relatório do TCU como sendo a média simples das notas dos 5 controles avaliados. A nota de cada controle também é a média simples das notas obtidas nas medidas de segurança do controle.

Quadro 15 – Nível/Faixa de Resultados ISegCiber

Nível	Faixa de resultados
Inexistente	iSegCiber <= 15
Inicial	15 < iSegCiber <= 50
Intermediária	50< iSegCiber <= 80
Aprimorado	iSegCiber > 80

Os resultados da avaliação da Conab apurados pela pesquisa foram:

Quadro 16 - Indicadores de Segurança Cibernética

Controle	Valor
1) Inventário e controle de ativos corporativos (icontrole 1)	43
2) **Inventário e controle de ativos de *softwares* (icontrole 2)**	20
3) Gestão contínua de vulnerabilidades (icontrole 7)	36
4) Conscientização sobre segurança e treinamento de competências (icontrole 14)	1
5) Gestão de resposta a incidentes (icontrole 17)	6
ISegCiber	21
InSegCiber	Inicial

Fonte: Audin a partir dos dados do Relatório do TCU

Analisando as respostas da Sutin e os resultados obtidos, destacam-se a seguir os pontos que mereceram atenção:

a) Em relação ao controle "Gestão contínua de vulnerabilidades", a pontuação ficou prejudicada principalmente pela avaliação das medidas de segurança "7.1. Estabelecer e manter um processo de gestão de vulnerabilidade" e "7.2. Estabelecer e manter um processo de correção de vulnerabilidades". Entre os principais achados da avaliação que justificam essa pontuação, selecionados e sintetizados por esta auditoria, tem-se que a Conab:

   i. Adota parcialmente um plano de gestão de vulnerabilidades, mas não possui um processo formalmente aprovado e documentado de gestão de vulnerabilidades;

   ii. O processo de gestão de vulnerabilidade não é revisado e atualizado anualmente (ou ainda mais frequentemente);

   iii. O processo de gestão de vulnerabilidades não define papéis e responsabilidades;

   iv. Não possui um processo formalmente aprovado e documentado de correção de vulnerabilidades; e

   v. As correções das vulnerabilidades identificadas não são priorizadas de acordo com os respectivos riscos.

b) O controle “Conscientização sobre segurança e treinamento de competências” obteve a pior avaliação entre os controles avaliados (nota 1). Apenas a medida “14.1 Estabelecer e manter um programa de conscientização em segurança” conseguiu a pontuação 6 e para as subquestões dessa medida, as respostas foram “não se aplica”. Para as demais medidas avaliadas (14.2 a 14.8), a Sutin informou não adotar, o que significa que não há treinamento dos colaboradores para os seguintes temas: reconhecimento de ataques de engenharia social[37] (14.2), em melhores práticas de autenticação de usuários (14.3), em melhores práticas de tratamento de dados (14.4), para evitarem exposição não intencional de dados (14.5), para reconhecerem e notificarem incidentes de segurança (14.6), para identificarem e notificarem a falta de atualização de ativos corporativos (14.7) e sobre os perigos de conectar-se e transmitir dados corporativos por meio de redes inseguras (14.8). Tais resultados levaram à pontuação 1 para o controle.
c) Para a avaliação do controle “Gestão de resposta a incidentes”, o TCU utilizou 3 medidas: 17.1 – Designar responsáveis por gerenciar o tratamento de incidentes, 17.2 – Estabelecer e manter contatos para reporte de incidentes de segurança e 17.3 Estabelecer e manter um processo de recebimento de notificações de segurança.

Para cada uma dessas medidas, a Sutin informou que “há decisão formal ou plano aprovado para adotar”[38]. Cada medida recebeu a nota 6[39], ficando a nota do controle como 6 (média das notas das 3 medidas).

Para esta avaliação do TCU, considerar que a avaliação foi feita em 2021 e a Equipe de Tratamento e Resposta a incidentes em Redes computacionais (ETTIR-Conab) veio a ser criada em 2022. O Ato de Criação desta equipe prevê avanços, como a existência de Canais de Atendimento:

> *A ETIR-Conab atenderá diretamente todas as unidades da Conab que registrarem suspeita ou eventos identificados como incidentes de segurança, preferencialmente, por meio de registro eletrônico de chamado no Sistema*

37 Manipulação psicológica de indivíduos para que executem ações que não deveriam ou então que divulguem informações confidenciais, sigilosas ou sensíveis

38 O grau de adoção da medida recebe as seguintes notas: 0- não adota ou não se aplica, 10 – há decisão formal u plano aprovado para adotar, 25- Adotado em menor parte, 50 – adotada parcialmente, 100 – Adotada em maior parte ou totalmente.

39 A nota da medida é uma média ponderada das questões tipo A com peso 60 e do tipo B, pelo 40. Como a nota do tipo A ficou 10 (vide a nota de rodapé n° 6) e a nota das questões tipo B foi 0 (pois foram respondidas como “não se aplica”), a nota final da medida foi 6.

de Gestão de Demandas - SIGEDE ou através do e-mail: seguranca@conab.gov.br.

Informa, ainda, o referido Ato que os incidentes devem ser categorizados por meio dos critérios que elenca.

A nota da Conab para o indicador iSegCiber ainda é modesta, indicando que a Companhia se encontra no estágio inicial (iSegCiber 21), compatível com as várias fragilidades apontadas pela avaliação. Acredita-se que esta avaliação possa ser utilizada pela Sutin como oportunidade para melhoria dos seus controles, servindo de insumos para a melhoria dos seus processos. Para o controle "Conscientização sobre segurança e treinamento de competências", por exemplo, cuja nota de avaliação foi muito baixa (nota 1), a implementação das medidas testadas na avaliação, envolvendo o treinamento de colaboradores em temas sensíveis de segurança cibernética, é factível, com boa relação custo/benefício, tendo impacto significativo no indicador e na segurança cibernética da Conab.

Em nova rodada de avaliação, provavelmente a nota final da Conab para o iSegCiber seria melhor que a atual, em virtude das mudanças já ocorridas desde a avaliação (2021) incentivada pelo Tribunal de Contas da União.

8.3 Conclusão

Com base na exposição anterior, temos a seguinte síntese dos achados:

i. A Equipe de Tratamento e Resposta a incidentes em Redes computacionais (ETIR-Conab) foi criada pelo ATO DE SUPERINTENDÊNCIA SUTIN N.º 8, conforme recomendação dos normativos pertinentes e a eles está alinhada. A Instrução Normativa 05/IN01/DSIC/GSIPR78 disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.
ii. Não foram informadas evidências quanto à efetiva implementação da ETIR-Conab. Trata-se de iniciativa relativamente recente, já que a ETIR-Conab é de recente instalação, vide data de sua criação (20/12/2022). A SA n°4 trouxe uma referência de sua atuação.

iii. O Ato de criação da ETIR-Conab trouxe a proposição de implementação de indicadores, o que é uma iniciativa relevante. Para os indicadores já propostos, sugerem-se ajustes e criação dos Acordos de Níveis de Serviço (SLA).

iv. As demandas do PCN para a SUTIN não foram implementadas (criação de plano de continuidade específico para os processos de TI), de forma integrada ao PCN e criação de um Time de Recuperação de Desastres (TRD- Sutin). Quanto à criação de um Time de Recuperação de Desastres (TRD- Sutin), o entendimento é que a ETIR-Conab, já criada conforme seu ato de Superintendência n° 08, pode vir a suprir as demandas do PCN, desde que implementados os eventuais ajustes que se fizerem necessários.

v. A partir da descrição feita pela Sutin, observa-se que esta possui processo de recuperação em caso de desastres definido, entretanto, ressente-se da formalização, institucionalização e normatização deste.

vi. Segundo a Sutin, quanto à ocorrência de incidentes que envolvam acesso indevido ao ambiente de TI no período entre 2019 e 2023, ocorreu apenas um incidente em 2019. Trata-se de um número pequeno, considerando o período analisado, e ocorreu por falhas nos controles.

vii. A nota da Conab para o indicador iSegCiber ainda é modesta, indicando estar no estágio inicial (iSegCiber = 21), compatível com as várias fragilidades apontadas pela avaliação. Os controles mais mal avaliados foram: a) Conscientização sobre segurança e treinamento de competências (*icontrole* 14); e b) Gestão de resposta a incidentes (*icontrole* 17).

À luz dos achados de auditoria sumarizados acima, sugere-se:

i. O Ato de criação da ETIR-Conab e as implicações das ações ali propostas deveria servir de insumo, em conjunto com as observações feitas por este Relatório de Auditoria, para a revisão e atualização da Norma de gestão de Serviços (NOC 60.214), quanto ao Processo de nível 2 “Realizar a Gestão da continuidade”, previsto na Cadeia de Valor, *vide* análise do Risco 4, no item 6 deste relatório.

ii. Ainda durante a revisão da NOC 60.214, esta deveria prever MAP específica para detalhamento dos processos e procedimentos referentes ao processo de gestão da continuidade, em particular com relação aos procedimentos para tratamento de

ataques cibernéticos, em conformidade com o conteúdo do Ato de criação da ETIR-Conab.

iii. Implementar o sistema de indicadores previstos no Ato de criação da ETIR-Conab, considerando as sugestões de melhorias indicadas neste Relatório.

iv. Considerando os apontamentos das fragilidades feitos no item 8.2.3 deste relatório, notadamente quanto aos controles: a) conscientização sobre segurança e treinamento de competências (*icontrole* 14); e b) gestão de resposta a incidentes (*icontrole* 17) recomenda-se a elaboração de planos de ação para os dois controles, com foco nas medidas mais mal avaliadas, objetivando a melhoria do processo de segurança da Informação.

v. Após a implementação destes planos de ação, realizar uma nova autoavaliação dos controles avaliados no Relatório do TCU, juntamente com a avaliação do controle "11 – Recuperação de dados", utilizando os mesmos critérios da avaliação feita pelo TCU, visando a melhoria do processo de Segurança da Informação. Elaborar relatório comparativo com os resultados obtidos com aqueles da avaliação feita pelo TCU, objetivando observar a evolução dos controles adotados e suas medidas entre as duas avaliações.

8.4 Comentários do Gestor

A seguir, inseriu-se os comentários do Gestor para o risco em análise, realizados após a apresentação deste Relatório:

Concordamos com as conclusões, entretanto discordamos quanto ao uso da metodologia do TCU como instrumento avaliativo. Como parte do processo de transformação digital, a Conab está utilizando um framework baseado no CIS-Controls, onde uma avaliação baseline foi realizada no final de 2023, com nova avaliação sendo realizada em fevereiro de 2024.

Concomitantemente a ação de implementar métricas relacionadas a maturidade de segurança de informação, estamos trabalhando na minuta de uma nova versão da política de segurança, que institui nos normativos da Companhia os papeis da ETIR, além de novas responsabilidades, referentes a segurança da informação, ao comitê gestor de segurança da informação.

Considerações da Audin acerca dos comentários do Gestor:

Há uma discordância, por parte da Sutin, referente a aspectos metodológicos, quando da adoção do Relatório do TCU "Acompanhamento de Controles Críticos de Segurança Cibernética das Organizações Públicas Federais" como instrumento avaliativo.

O argumento da Sutin é que a Conab está utilizando um framework baseado no CIS-Controls.

Ocorre que o referido relatório do TCU, que serviu de base para a análise, também adotou o framework CIS como base para elaboração do questionário da pesquisa realizada, conforme se pode observar em extrato deste relatório, pagina 2:

> *O questionário foi elaborado com base na versão 8 do framework do Center for Internet Security (CIS), que prevê um total de dezoito controles críticos de SegCiber, subdivididas em 153 medidas de segurança: 53 básicas, 74 intermediárias e 23 avançadas.*

9 Conclusões

O relatório apresentou a análise dos 6 riscos selecionados como de magnitude extrema ou grave, dentre os 13 identificados, envolvendo a disponibilidade dos serviços de TI, na Conab.

Ressalte-se que, destes 6 riscos, 4 são relativos a processos de trabalhos (riscos 3, 4, 5 e 6), os quais se caracterizam pela baixa maturidade da maioria deles, notadamente quanto à definição, normatização e institucionalização. O relatório teve a preocupação de apontar este estágio de maturidade, identificar as fragilidades e as oportunidades de melhorias. A percepção é que estes riscos significam, em última análise, os maiores desafios para a Sutin, no sentido de que demandarão muito esforço, tempo, dedicação e apoio da Companhia para o cumprimento das sugestões propostas.

Quando aos outros dois riscos analisados, o risco 1 tratou da utilização de ativos de TI sem garantia, sendo que a análise demonstrou que a situação é menos grave que a avaliação inicial do risco apontou, e que as soluções já haviam sido convenientemente encaminhadas pela Sutin.

Quando ao risco 2, relativo Investimentos insuficientes em ferramentas e infraestrutura de TI, a surpresa foi positiva quanto à contratação dos serviços de TI. A Sutin vem utilizando o PDTI como instrumento prioritário de planejamento das aquisições de Tecnologia da Informação, indicando que aquisições não programadas ocorram apenas em situação de excepcionalidade, embora tenham sido identificadas oportunidades de melhorias quanto à elaboração destes instrumentos.

Por fim, esperamos que o relatório venha a contribuir para a melhoria dos serviços prestados pela Sutin, por meio da análise de oportunidade e conveniência dos gestores da Sutin na implementação das sugestões propostas.

10 Anexos

Anexos I

Propostas orçamentárias previstas nos Instrumentos de Planejamento (PDTI 2015-2018)

Proposta Orçamentária 2015 – Custeio:

Especificação dos contratos	Total
Acesso à Rede SERPRO através do SNA Server – Proc. 769/2011	11.331,84
Links de comunicação de Dados: Matriz, Bolsa de Mercadorias, SUREG's e Unidades Armazenadoras - Proc. 1002/2009	5.002.426,92
Contratação da Infovia (SERPRO). Processo 1269/2014, em substituição ao proc. 2483/2012.	348.000,00
Manutenção preventiva/corretiva de equipamentos. Processo 1571/2011	180.000,00
Helpdesk e atualização de versão do SAAGRA – KM&M – Proc. 2170/2007.	656.305,04
Suporte, atualização de versão e manutenção evolutiva do Sistema de Gestão de Recursos Humanos – Vetorh Proc. 1332/2009	672.000,00
Acesso à CETIP via RTM (Acesso discado) - Proc. 1252/2010	7.200,00
Manutenção da sala cofre. Proc. 2298/2011	384.000,00
Manutenção do Storage. Proc. 2124/2012	28.200,00
Aquisição de licenças de uso e atualização de solução antivírus e antispyware corporativos. Proc. 2316/2010	80.000,00
Aquisição/atualização de *softwares* para atendimento às demandas da área meio da Companhia (SUPAD, SUCON, SUOFI etc)	700.000,00
Projeto implantação de Plano de Continuidade de Negócio Excel_BuiltIn_Print_Area_4_1 Gestão de risco. Proc. nº 1181/2014	1.000.000,00
Suporte e atualização de licenças de uso, implantação e suporte técnico de ferramenta de Gerenciamento remoto de estações de trabalho. Go-Global	6.000,00
***Software* de Gerenciamento de ativos de rede**	64.000,00
Aquisição *software* para atendimento à GEOTE	460.000,00
Circuito Contingência Internet	300.000,00
Acesso Internet 1MB (OpenDF)	3.180,00
Total	**9.902.643,80**

Fonte: PDTI 2015-2018

Proposta Orçamentária 2015 – Investimento:

Descrição do Equipamento	Quantidade	Valor
- Renovação do parque computacional (UAs, SUREGs e Matriz): - microcomputadores	2.500	6.500.000,00
- Impressoras Laser (27 ppm)	260	208.000,00
- Impressoras Multifuncionais Coloridas	580	986.000,00
- Notebooks/Netbooks	200	700.000,00
- Scanners de produção (30 ppm)	140	420.000,00
- Tablets	200	360.000,00
- Switches (concentradores de rede)	424	992.740,00
- Servidores de rede	27	675.000,00
- Servidores corporativos	6	420.000,00
- Sistema automático de *Backup*	1	70.000,00
- GBIC SFP+ 10Gbps	129	77.400,00
- Módulo SFP+ 1Gbps	10	30.810,00
- Placa de Rede 10gbps Single Porte	20	53.400,00
- Solução VoIP (Equipamentos)	1	4.200.000,00
- Solução Videoconferência (Equipamentos)	1	2.400.000,00
- Cofres Geocatálogos / 172 fitas / 12 HDs		103.000,00
- Fluck (Certificador de rede)	1	60.000,00
Pacote *softwares* Microsoft		
- Windows Server	100	275.989,00
Cal 4	300	346.451,00
- Cal Internet	1	6.469,50
- SQL Server	10	112.100,00
- Office	300	476.700,00
- Project	12	26.190,00
Computador MacBook Air 11 polegadas para desenvolvimento de aplicativos Mobile	2	12.000,00
Smart TV 55” para reuniões	1	4.000,00
Datashow	4	16.000,00
Total		**19.532.249,50**

Fonte: PDTI 2015-2018

Proposta Orçamentária 2016 – Custeio

Especificação dos contratos	Total
Acesso à Rede SERPRO através do SNA Server – Proc. 769/2011	11.331,84
- Links de comunicação de Dados: Matriz, Bolsa de Mercadorias, SUREG's e Unidades Armazenadoras – Proc. 2936/2013	8.352.000,00
- Acesso à Infovia (SERPRO). Processo 1269/2014	348.000,00
- Manutenção preventiva/corretiva de equipamentos. Processo 1571/2011	120.000,00
- Atualização de versão e suporte técnico ao SAAGRA – KMM – Proc. 0741/2013	656.305,04
- Suporte, atualização de versão e manutenção evolutiva do Sistema de Gestão de Recursos Humanos – Vetorh. Proc. 2243/2014	672.000,00
- Acesso à CETIP via RTM (Acesso discado) - Proc. 594/2015	26.584,56
- Manutenção da sala cofre. Proc. 2298/2011.	391.878,84
- Manutenção do Storage. Proc. 2124/2012	28.200,00
- Aquisição de licenças de uso e atualização de solução antivírus e antispyware corporativos. Processo 2316/2010 em andamento.	12.000,00
- Aquisição de licenças de uso e atualização de solução antivírus e antispyware corporativos. Nova contratação	200.000,00
- Aquisição/atualização de *softwares* para atendimento às demandas da área meio da Companhia (SUPAD, SUCON, SUOFI etc.)	700.000,00
- Projeto implantação de Plano de Continuidade de Negócio Excel_BuiltIn_Print_Area_4_1 Gestão De risco. Proc. nº 1181/2014	1.000.000,00
- Suporte e atualização de licenças de uso, implantação e suporte técnico de ferramenta de gerenciamento remoto de estações de trabalho.	10.000,00
- Licenças de sistema operacional Windows Server, SGBD SQL Server, Ferramentas de escritório e *software* processamento de imagem	500.000,00
- Licença de uso anual Mapas empresa Maplink	24.000,00
- Licença para desenvolvimento iOS (Apple)	350,00
- Atualização Base de Endereçamento dos Correios	2.500,00
Licença para desenvolvimento Windows Mobile	160,00
TOTAL	**13.055.310,28**

Fonte: PDTI 2015-2018

Proposta Orçamentária 2016 – Investimento:

Descrição do Equipamento	Quantidade	Valor
- Microcomputadores	1.200	4.200.000,00
- Impressoras Laser	40	48.000,00
- Impressoras Multifuncionais Coloridas	10	40.000,00
- Impressoras Multifuncionais Monocromáticas	45	90.000,00
- Notebooks/Netbooks	120	480.000,00
- Scanners de produção	60	210.000,00
- Tablets.	800	1.600.000,00
- Switches (concentradores de rede)	50	140.000,00
- Servidores de rede	120	3.000.000,00
- Servidores corporativos	6	480.000,00
- Sistema automático de *Backup*	1	70.000,00
- Solução VoIP (Equipamentos)	1.	4.200.000,00
- 2 Cofres Geocatálogos, 172 fitas e 12 HDs	1	150.000,00
- Fluck (Certificador de rede)	1	90.000,00
- Computador MacBook Air 11 polegadas para desenvolvimento de aplicativos Mobile	2	12.000,00
- Smart TV 55" - Salas de reuniões	2	8.000,00
TOTAL		**14. 818.000,00**

Fonte: PDTI 2015-2018

PDTIC 2021-2024

Neste documento, o item 12 – Plano orçamentário apresenta o Plano de Investimentos 2021 aprovado pelo CETI em sua 27a reunião ordinária, realizada em 24/03/2021, transcrita a seguir:

Plano de Investimentos 2021

ID	Descrição	I	C
1	Aquisição de Webcams com microfone embutido, USB	60.000	
2	Ferramenta de produtividade, colaboração e comunicação	1.226.400	
3	Atualização do parque tecnológico (micros, notebooks e outros equipamentos)	3.510.000	
4	Bilhetagem e Monitoramento de Impressão (*Software*)	12.000	
5	Bibliotecas (Arquitetura de *software*)	30.000	
6	Equipamento para realização de *Backup*	469.203	
7	Extensão do suporte técnico cerne da rede (Switchcore)		265.550
8	Renovação do Contrato N.º 08/2018 para a manutenção de equipamentos		120.894
9	Renovação do Contrato N.º 21/2017 que trata do suporte técnico de Antivírus		44.342
10	Renovação do Contrato N.º 14/2016 que trata do fornecimento de Internet SERPRO		428.194
11	Contratação INFOVIA SERPRO		141.600
	Outsourcing de Impressão - SEDE		560.160
13	Tarifador telefônico (Info360)		7.576
14	Extensão do suporte técnico da solução VoIP		800.000
15	Aquisição de cartuchos para solução de *backup* (integrado ao item *Backup*)		16.000
16	Solução de Prevenção de perda de dados (DLP)		589.531
	Total	**5.307.603**	**3.631.047**
	Total Geral	**8.938.650**	

Legenda: I - Investimento; e C - Custeio. (Foram suprimidos os centavos)

Fonte: PDTIC 2021-2024

Anexo II – Aquisições de bens e Serviços de TI - 2015-2023

Ano	Nº Contrato	Objeto	Início	Fim	Valor Total	Origem
2015	003	Serviços de suporte, manutenção e atualização de versão para 2 (duas) licenças *software* ACL Windows Desktop.	02/23/2017 ???	02/23/2016 ???	R$ 14.616,00	PDTIC 2015-2018
2015	003	TA1	02/23/2016	02/23/2017	R$ 6.685,72	PDTIC 2015-2018
2015	020	Aquisição de biblioteca de fitas por meio de adesão à ata de registro de preços nº 66/2013 do Exército Brasileiro - Comando Militar do Sul.	02/10/2015	02/09/2016	R$ 175.000,00	PDTIC 2015-2018
2015	025	Aquisição de módulo para biblioteca de fitas e 20 unidades de fitas LTO-6. Aquisição complementar à OC 20/2015. Adesão à ata de registro de preços Nº 66/2013 do Exército Brasileiro – Comando Militar do Sul.	02/23/2015	02/22/2016	R$ 23.100,00	PDTIC 2015-2018
2015	015	Aquisição de 880 impressoras, conforme requisitos técnicos constantes do Termo de Referência.	09/21/2015	09/20/2016	R$ 1.471.202,00	PDTIC 2015-2018
2015	018	Aquisição de solução VOIP, com manutenção, conforme Cláusula Primeira do Contrato e Termo de referência.	12/14/2015	12/11/2016	R$ 1.707.531,76	PDTIC 2015-2018
2015	022	Aquisição de licenças de *software* Microsoft. Windows Server 2012, Windows Server 2012 Dvc Cal, Windows Server 2012 Ext Conn, SQL Server 2014.	12/18/2015	12/17/2016	R$ 658.212,80	PDTIC 2015-2018
2015	023	Aquisição de 300 licenças de *software* Microsoft Office.	12/28/2015	12/27/2016	R$ 476.700,00	PDTIC 2015-2018
2015	025	Fornecimento de 665 Microcomputadores HP Desktop com Windows	12/29/2015	12/29/2020	R$ 2.659.933,50	PDTIC 2015-2018
2015	013	Contratação de empresa especializada em manutenção preventiva e corretiva de 03 nobreaks instalados na Sutin durante 03 meses.	04/02/2015	07/01/2015	R$ 5.400,00	PDTIC 2015-2018
2016	007	Contrato emergencial Rede de longa distância (WAN) com a Claro S/A.	06/11/2016	12/08/2016	R$ 2.394.476,16	PDTIC 2015-2018
2016	012	Contratação para solução de serviços de telecomunicações, por rede IP (Internet Protocol) multisserviços, com tecnologia MPLS, para prover tráfego de voz, dados e imagem, no âmbito de toda Companhia.	06/01/2016	12/01/2018	R$ 10.231.308,00	PDTIC 2015-2018
2016	012	TA1[40]	12/01/2018	05/31/2021	R$ 10.231.308,00	PDTIC 2015-2018
2016	012	Prorrogação Excepcional	06/01/2021	05/31/2022	R$ 3.191.697,24	PDTIC 2015-2018
2016	011	Contratação de solução em serviços de telecomunicações, por meio de circuito dedicado de acesso Internet, para interconexão entre a Matriz da Companhia e a rede mundial de computadores - a Internet.	06/01/2016	12/01/2018	R$ 433.589,10	PDTIC 2015-2018
2016	011	TA1	12/01/2018	05/31/2021	R$ 390.230,10	PDTIC 2015-2018
2016	014	Serviços de Tecnologia da Informação e Gerenciamento de Conexões à Rede Infovia Brasília, conforme modelo de negócios.	10/23/2016	10/22/2017	R$ 387.809,76	PDTIC 2015-2018
2016	014	TA1	10/23/2017	10/22/2018	R$ 397.347,00	PDTIC 2015-2018

40 TA se refere a Termo Aditivo (Nota da Audin)

2016	014	TA2	10/23/2018	10/22/2019	R$ 413.998,08	PDTIC 2015-2018
2016	014	TA3	10/23/2019	10/22/2020	R$ 428.193,24	PDTIC 2015-2018
2016	014	TA4 e Apostilamento[41]	10/23/2020	10/22/2021	R$ 324.409,84	CETI (6ª Reunião Extraordinária)
2016	019	Aquisição de 341 microcomputadores, conforme especificações constantes da ARP /UFBA.	12/22/2016	12/21/2017	R$ 1.431.859,00	PDTIC 2015-2018
2016	022	Contrato emergencial, para prestação de serviço de comunicação de dados, voz videoconferência entre Matriz e Superintendências, com validade de 180 dias, a partir de 08.12.2016, improrrogáveis e irreajustáveis.	12/08/2016	06/06/2017	R$ 304.082,52	PDTIC 2015-2018
2017	021	Aquisição de novas licenças para atualização da solução de uso perpétuo de antivírus Mcafee, visando a instalação, configuração, garantia, assistência técnica destas novas licenças, e ainda, a renovação e atualização de licenças já existentes, assim como a renovação do Contrato dos serviços de suporte técnico e gerenciamento on site da solução.	07/31/2017	07/30/2018	R$ 403.920,00	PDTIC 2015-2018
2017	021	TA1	07/31/2018	07/30/2019	R$ 43.867,20	PDTIC 2015-2018
2017	021	TA2	07/31/2019	07/30/2020	R$ 43.867,20	PDTIC 2015-2018
2017	021	TA3	07/31/2020	07/30/2021	R$ 43.867,20	CETI (6ª Reunião Extraordinária)
2017	021	TA4	07/31/2021	07/30/2022	R$ 43.867,20	PDTIC 2015-2018
2018	010	Fornecimento, mediante registro de preços, de equipamento visando a expansão da solução VoIP existente, para atendimento das necessidades da Conab.	03/26/2018	09/25/2018	R$ 1.661.021,64	PDTIC 2015-2018
2018	008	Contratação de empresa especializada na manutenção corretiva e preventiva dos equipamentos de informática da Matriz, CDRH e SUREG-DF	06/01/2018	05/31/2019	R$ 181.340,40	PDTIC 2015-2018
2018	008	TA1	06/01/2019	05/31/2020	R$ 181.340,40	PDTIC 2015-2018
2018	008	TA2	06/01/2020	05/31/2021	R$ 120.893,52	CETI (6ª Reunião Extraordinária)
2018	008	TA3	06/01/2021	05/31/2022	R$ 120.893,52	PDTIC 2021-2024
2018	008	TA4	06/01/2022	05/31/2023	R$ 141.430,12	PDTIC 2021-2024
2018	017	Aquisição de 2 cofres para mídia magnética	07/09/2018	01/08/2019	R$ 87.159,94	PDTIC 2015-2018
2018	OC 119/2018	Aquisição de 2 iMAC Apple e 2 Ipads	12/18/2018	12/18/2019	R$ 18.199,98	CETI (citada na 19a reunião)
2018	025	Extensão de Suporte técnico para Oracle StorageTek SL150 e sua respectiva expansão de módulo.	10/18/2018	10/17/2023	R$ 10.812,00	PDTIC 2015-2018
2019	OC 011/2019	Aquisição de 8 notebooks para CONSAD	02/25/2019	02/25/2020	R$ 49.111,68	CONSAD

41 Segundo o RLC, apostilamento contratual é: registro, previamente autorizado pela autoridade competente, tendo por objetivo a anotação da variação do valor contratual para fazer face ao reajustamento de preços previsto no próprio Contrato, as atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento nele estabelecidas, correção de erros materiais e outros dispositivos previstos neste Regulamento. (Nota da Audin)

2019	051	Aquisição de 48 cilindros Drum Okidata para impressoras OKIDATA modelo OKI MB491+ e OKI B431dn.	12/11/2019	12/11/2020	R$ 15.000,00	
2019	005	Contratação de empresa especializada para prestação de SERVIÇOS DE MANUTENÇÃO EM SALA-COFRE, certificada segundo as normas técnicas ABNT/NBR 15.247 e ABNT/NBR 60.529.	02/08/2019	02/08/2024	R$ 506.874,69	PDTIC 2015-2018
2019	005	Apostilamento	11/01/2019	02/08/2024	R$ 515.498,76	PDTIC 2015-2018
2019	005	Apostilamento	11/01/2020	02/08/2024	R$ 520.548,33	PDTIC 2015-2018
2019	005	Apostilamento	11/01/2021	02/08/2024	R$ 549.990,33	PDTIC 2021-2024
2019	005	Apostilamento	11/01/2022	02/08/2024	R$ 602.459,91	PDTIC 2021-2024
2020	OC 042/2020	Aquisição de 25 cilindros para impressoras OKIDATA modelo OKI MB491+ e OKI B431dn.	09/24/2020	09/24/2021	R$ 5.325,00	
2020	010	Contratação de extensão de garantia e suporte, por 60 (sessenta) meses, para equipamento do tipo Switch Core.	04/03/2020	04/02/2025	R$ 260.000,00	CETI (6ª Reunião Extraordinária)
2020	008	Contrato de fornecimento de 6 (seis) licenças de uso de Softwre na Nuvem (*Software* as a Service - Saas) Microsoft Power BI e Capacitação da Ferramenta.	05/07/2020	05/07/2021	R$ 2.999,00	PDTIC 2015-2018
2020	011	Aquisição de bens do tipo "Servidor de Rede" conforme especificações, condições, quantidades e exigências detalhadas no contrato e estabelecidas no termo de referência - anexo I, do edital do pregão eletrônico Conab nº 17/2019.	05/22/2020	05/22/2021	R$ 944.592,00	PDTIC 2015-2018
2021	001	Aquisição de bens do tipo "Servidor de Rede" conforme especificações, condições, quantidades e exigências detalhadas no contrato e estabelecidas no termo de referência - anexo I, do edital do pregão eletrônico Conab nº 17/2019.	02/12/2021	02/11/2022	R$ 95.499,00	PDTIC 2015-2018
2021	005	Aquisição de equipamento do tipo Switch Fibre Channel, conforme especificações, condições, quantidades e exigências detalhadas neste Contrato e estabelecidas no Termo de Referência - Anexo I, do Edital de Pregão Eletrônico Conab nº 11/2020.	03/17/2021	09/16/2021	R$ 134.994,42	CETI (6ª Reunião Extraordinária)
2021	004	Aquisição de solução de armazenamento de dados - Storage, conforme especificações, condições, quantidades e exigências detalhadas neste Contrato e estabelecidas no Termo de Referência - Anexo I, do Edital de Pregão Eletrônico Conab nº 11/2020.	03/03/2021	09/02/2021	R$ 263.000,00	CETI (6ª Reunião Extraordinária)
2021	013	Contratação de solução de comunicação de dados composta por SD-WAN (*Software* - defined Networking in a Wide Area Network) capaz de prover a interconexão da Matriz da Conab, suas superintendências regionais, suas unidades armazenadoras e as bolsas de mercadoria, entre si e com a Internet, em âmbito nacional, e acesso redundante à Internet, na Matriz.	06/08/2021	06/07/2026	R$ 13.178.230,20	PDTIC 2021-2024
2021	014	Contratação de solução de comunicação de dados composta por SD-WAN (*Software* - defined Networking in a Wide Area Network) capaz de prover a interconexão da Matriz da Conab, suas superintendências regionais, suas unidades armazenadoras e as bolsas de mercadoria, entre si e com a Internet, em âmbito nacional, e acesso redundante à Internet, na Matriz.	07/01/2021	06/30/2026	R$ 18.873,48	PDTIC 2021-2024
2021	014	TA1	06/22/2022	06/30/2026	R$ 17.693,91	PDTIC 2021-2024

2021	014	TA2	02/15/2023	06/30/2026	R$ 73.446,75	PDTIC 2021-2024
2021	017	Fornecimento de 17 [dezessete] licenças de uso de *software* na nuvem [*Software* as a Service - SaaS] Microsoft Power BI, conforme especificações, condições, quantidades e exigências estabelecidas no Termo de Referência	06/29/2021	06/30/2022	R$ 10.962,96	PDTIC 2021-2024
2021	025	A prestação de serviço de tecnologia da informação para monitoração, gerenciamento e suporte às conexões à Infovia Brasília.	10/23/2021	10/23/2026	R$ 141.600,00	CETI (27ª Reunião)
2021	025	Apostilamento	10/23/2022	10/23/2026	R$ 607.004,16	PDTIC 2021-2024
2022	007	Contratação de serviços de garantia e suporte técnico para a solução de telefonia VoIP da Conab - Avaya Aura, da fabricante Avaya.	03/25/2022	03/25/2023	R$ 560.000,00	PDTIC 2021-2024
2022	007	TA1	03/25/2023	03/25/2024	R$ 560.000,00	PDTIC 2021-2024
2022	023	Aquisição de 60 cilindros Drum Okidata P/N - 44574301 para impressoras OKIDATA modelo OKI MB491+ e OKI B431dn.	21/06/2022	19/09/2022	R$ 6.648,60	CETI (6ª Reunião Extraordinária)
2022	028	Contratação de Solução de Antivírus e Prevenção de perda de dados – DLP da McAfee, com suporte e garantia do fabricante e treinamento técnico especializado.	08/23/2022	08/23/2027	R$ 1.349.709,60	PDTIC 2021-2024
2022	020	O objeto do presente Contrato é o fornecimento de 17 [dezessete] licenças de uso de *software* na nuvem [Software as a Service - SaaS] Microsoft Power BI, conforme especificações, condições, quantidades e exigências estabelecidas no Termo de Referência.	07/26/2022	07/25/2023	R$ 11.364,84	PDTIC 2021-2024
2023	018	Aquisição de estações de trabalho (desktops) e notebooks.	05/23/2023	05/22/2024	R$ 1.199.940,00	PDTIC 2021-2024
2023	019	Aquisição de Worksations.	05/16/2023	06/15/2024	R$ 391.000,00	PDTIC 2021-2024
		Total			R$ 63.453.537,76	

Fonte: Sutin

11 Referências

Associação Brasileira de Normas Técnicas (ABNT). **Norma NBR ISO/IEC 17799**. Rio de Janeiro – RJ. 2005.

Center for Internet Security. **Controles CIS Versão 8**. 2021. Disponível em < https://www.cisecurity.org/controls/v8>. Acesso em 14/12/2023.

Conab – **COMPANHIA NACIONAL DE ABASTECIMENTO. Regimento Interno – NOC 10.104**. Brasília. 2018. Disponível em < https://www.conab.gov.br/images/arquivos/normativos/10000_sistema_institucional/10.104_RI_24_8_23_47_versao_1.pdf >. Acesso em 14/12/2023.

_____. **Norma de Gestão de Serviços de Tecnologia da Informação (TI) – NOC 60.214**. Brasília. 2021. Disponível em < https://www.conab.gov.br/images/arquivos/normativos/60000_sistema_de_administracao/60.214_norma_gestao_servicos_tecnologia_informacao.pdf>. Acesso em 14/12/2023.

_____. **NORMA DE RECURSOS COMPUTACIONAIS -60.213**. Disponível em <https://www.conab.gov.br/images/arquivos/normativos/60000_sistema_de_administracao/60.213_Norma_de_Recursos_Computacionais.pdf>. Acesso em 14/12/2023.

_____. Política de Segurança da Informação – 10.010. Disponível em <https://www.conab.gov.br/institucional/normativos/politicas-planos-e-cartas>. Acesso em 14/12/2023.

_____. **REGULAMENTO DE LICITAÇÕES E CONTRATOS DA CONAB (RLC) 10.901**. Disponível em <https://www.conab.gov.br/images/arquivos/normativos/10000_sistema_institucional/10.901_RLC_.pdf>. Acesso em 14/12/2023.

_____. **Plano Diretor de Tecnologia da Informação 2015-2018**.

_____. **Plano Diretor de Tecnologia da Informação e Comunicação PDTIC 2021-2024**. Disponível em <https://intranet.conab.gov.br/images/arquivos/PDTIC-2021-2024.pdf>. Acesso em 14/12/2023.

_____. **Cadeia de Valor**. Disponível em <https://www.conab.gov.br/participacao-social/conselhos-e-orgaos-colegiados/conselho-de-administracao/item/17295-resolucao-consad-n-021-de-16-12-2021-pdf>. Acesso em 14/12/2023.

Tribunal de Contas da União. **Acompanhamento de controles críticos de segurança cibernética das organizações públicas federais – Relatório Individual de Feedback – Conab (TC-036.301/2021-3, Acórdão 1768/2022-TCU-Plenário).** Brasília. Março de 2022.

Committee of Sponsoring Organization of the Deadway Commission (COSO). **COSO - Controle Interno - Estrutura Integrada**. 2013.