GRUPO tagGrupo – CLASSE V – tagColegiado
TC 036.620/2020-3
Natureza: Relatório de Auditoria.
Órgãos/Entidades: vários.

**SUMÁRIO: AUDITORIA SOBRE OS PROCEDIMENTOS DE BACKUP DAS ORGANIZAÇÕES PÚBLICAS FEDERAIS. DETERMINAÇÃO. RECOMENDAÇÃO. CIÊNCIA.**

RELATÓRIO

Adoto como parte integrante da presente decisão o relatório de fiscalização elaborado no âmbito da Secretaria de Fiscalização de Tecnologia da Informação (peça 898), que contou com parecer favorável da chefia imediata (peça 899) e da unidade técnica (peça 900), a seguir transcrito:

**"Introdução**

1. Trata-se de fiscalização do tipo auditoria, conforme previsto no art. 239 do Regimento Interno do Tribunal de Contas da União (RI/TCU)[i], conduzida de acordo com o "Manual de Auditoria Operacional", documento aprovado por meio da Portaria - Segecex 18/2020[ii]. Para a expedição das propostas de encaminhamento, foi devidamente observada a Resolução - TCU 315/2020[iii].

1.1. Decisão que originou a fiscalização

2. No âmbito da Estratégia de Fiscalização do TCU em Segurança da Informação (SegInfo) e Segurança Cibernética (SegCiber), cuja divulgação foi autorizada por meio do Acórdão 4.035/2020-TCU-Plenário (Rel. Min. Vital do Rêgo)[iv], foi prevista a realização, ainda em 2020, de uma "Auditoria sobre *backup*" (TC 001.873/2020-2, peça 46, Figura 37).

3. Essa fiscalização, então, foi autorizada por meio do Acórdão 2.737/2020-TCU-Plenário, de relatoria do Ministro-Substituto Marcos Bemquerer em substituição ao Ministro Vital do Rêgo[v] (TC 034.004/2020-3, peça 6).

1.2. Identificação do objeto

4. Efetividade dos procedimentos de *backup* e *restore* das organizações públicas federais.

1.3. Objetivo e escopo da auditoria

5. O objetivo do trabalho foi avaliar se os procedimentos de *backup* e *restore* das organizações da APF, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados.

6. Em especial, foram analisados aspectos relacionados à realização de cópias de segurança (*backups*) da principal base de dados tratada diretamente por cada organização e do servidor ou conjunto de servidores/máquinas de cada organização que hospedam o principal sistema cuja gestão está sob sua responsabilidade. Adicionalmente, foi verificada a execução periódica de testes de restauração (*restore*) sobre esses *backups*, a existência de mecanismos de proteção física e lógica sobre os respectivos arquivos e a guarda de ao menos uma instância dessas cópias em mídias não acessíveis remotamente e, portanto, protegidas de ações cibernéticas diretas, a exemplo dos ataques de *ransomware* ("sequestro" de dados).

7. Para melhor organização do conteúdo, esta auditoria foi estruturada a partir das respostas a cinco questões de auditoria (Anexo II - Planejamento da fiscalização), a saber:

7.1. Q1) A organização realiza, de forma regular e automática, cópias de segurança (*backups*) da sua principal base de dados?

7.2. Q2) A organização realiza, regularmente, cópias de segurança (*backups*) integrais (*e.g.* cópia da imagem) dos servidores/máquinas que hospedam seu principal sistema?

7.3. Q3) A organização realiza, periodicamente, testes de restauração (*restore*) das cópias de segurança (*backups*) citadas nas questões anteriores?

7.4. Q4) A organização implementa mecanismos de controle de acesso físico (*e.g.* sala cofre) e lógico (*e.g.* criptografia) para proteger as cópias de segurança (*backups*)?

7.5. Q5) A organização armazena as cópias de segurança (*backups*) em ao menos um destino não accessível remotamente?

8. Cada uma dessas questões de auditoria correspondeu a um grupo de perguntas específicas em questionário que foi aplicado, de forma *online*, a um total de 422 organizações públicas federais (Anexo I - Questionário da Auditoria sobre *backup*).

1.4. Processos conexos

9. O TC 001.873/2020-2 (Rel. Min. Vital do Rêgo)[vi] consiste em levantamento da governança e gestão de segurança da informação e de segurança cibernética da APF.

1.5. Métodos utilizados

10.O trabalho foi conduzido em conformidade com as Normas de Auditoria do TCU – NAT (Portaria - TCU 280/2010[vii], alterada pela Portaria - TCU 168/2011[viii]) e com o Manual de Auditoria Operacional do TCU (Portaria - Segecex 18/2020[6]) e está alinhado aos Princípios Fundamentais de Auditoria do Setor Público, conforme tradução da ISSAI 100, disponibilizada pelo portal do TCU[ix].

11.A metodologia utilizada, que consiste em mobilizar os próprios gestores para avaliarem seus controles e riscos, tipicamente por meio da aplicação de questionários ou da realização de oficinas de autoavaliação das práticas existentes para lidar com os riscos envolvidos, é chamada de autoavaliação de controles internos (CSA).

12.Em uma CSA típica, a auditoria atua como facilitadora do processo como um todo: coordena a elaboração do(s) instrumento(s) de coleta, orienta os gestores sobre o respectivo preenchimento, aplica o questionário para capturar os dados das autoavaliações, analisa esses resultados para identificar pontos que mereçam atenção e, ao final, realiza devolutivas (informação de *feedback*) com vistas a permitir que, por conta própria, as organizações sejam capazes de planejar a implementação das melhorias que considerem mais relevantes, de acordo com suas necessidades, realidades e contextos específicos[x].

13.A auditoria foi construída tomando por base os subcontroles do controle 10 (*Data Recovery Capabilities*) do *framework* de segurança cibernética do CIS. O questionário (Anexo I - Questionário da Auditoria sobre *backup*), apesar de essencialmente declarativo, instava o respondente a anexar evidências para suportar as principais respostas fornecidas, com vistas a melhorar sua confiabilidade, de modo geral. Essas evidências foram efetivamente verificadas pelos auditores para identificar possíveis incongruências nas respostas. Registre-se, contudo, que, mesmo nessas situações, as respostas fornecidas pelos gestores foram mantidas inalteradas.

14.As interações com as organizações auditadas se deram no bojo da plataforma utilizada para aplicação do questionário (LimeSurvey, versão 2.00+ Build 130929), à exceção do encaminhamento dos ofícios de comunicação da auditoria, realizado pela Secretaria de Gestão de Processos (Seproc) via Sistema Conecta, e do esclarecimento de dúvidas recebidas por *e-mail* ou por telefone.

15.Uma vez definidos, na fase de planejamento, os objetivos da auditoria e a forma como ela seria conduzida, foram elaboradas cinco macroquestões para nortear o trabalho (parágrafos 7.1-7.5; Anexo II - Planejamento da fiscalização). Cada uma dessas macroquestões foi, então, subdividida em conjuntos de perguntas específicas, as quais foram encadeadas para formar o questionário *online* que foi disponibilizado para ser respondido pelos gestores designados por cada organização.

16.O Capítulo 2 deste relatório reflete a forma com que a auditoria e, consequentemente, o questionário foram estruturados. Após uma parte inicial com o objetivo de aferir o porte da organização (quantidades de colaboradores, total e apenas do setor de TI) e verificar a existência de política de *backup* (Seção 2.1), seguem-se cinco seções de perguntas específicas, cada uma relacionada a um dos cinco subcontroles avaliados (Seções 2.2 a 2.6), além de outra para que os gestores avaliassem, eles próprios, as respectivas organizações em relação a esses subcontroles (Seção 2.7). Assim, o panorama geral das organizações públicas federais auditadas é apresentado ao longo das diferentes seções desse capítulo.

17.O Capítulo 3 descreve o painel (*dashboard*) que foi construído no âmbito desta auditoria para permitir a visualização gráfica e interativa das respostas das organizações, inclusive com a possibilidade de segmentação das análises a partir da aplicação de filtros diversos. Todas as figuras que ilustram o Capítulo 2, por exemplo, foram obtidas a partir desse painel.

18.A seu turno, o Capítulo 4 explica os propósitos desta auditoria, voltados tanto aos gestores das organizações auditadas quanto ao próprio TCU e aos dezessete auditores participantes, e comenta sobre os dois tipos de relatórios de *feedback* (individuais e comparativos) preparados para envio às organizações que responderam o questionário, de modo a ajudá-las a melhorar os subcontroles avaliados. Esse capítulo também descreve o indicador (iBackup) criado no âmbito da auditoria com a intenção de fornecer uma medida quantitativa à qualidade dos procedimentos de *backup*/*restore* das organizações.

19.O Capítulo 5 registra exemplos de boas práticas identificadas entre as organizações auditadas, as quais podem vir a ser copiadas por outros gestores. O Capítulo 6 apresenta informações complementares, como relatos de incidentes de segurança da informação significativos ocorridos durante a execução da auditoria e relacionados ao seu objeto, bem como uma síntese da atuação do Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) na coordenação das respostas a tais incidentes, além dos comentários mais relevantes feitos pelos respondentes do questionário e das avaliações que estes forneceram acerca da condução em si da auditoria.

20.O Capítulo 7, então, traz uma perspectiva para o futuro, sugerindo outros controles do *framework* do CIS cuja avaliação poderá ser priorizada pela Sefti ao longo dos próximos anos, no escopo da Estratégia de Fiscalização do TCU em SegInfo e SegCiber, cuja aprovação, proposta neste trabalho, mostra-se fundamental para o acompanhamento, pelo Tribunal, de tema tão relevante na APF.

21.Por fim, o Capítulo 8 apresenta a conclusão desta auditoria, enquanto o Capítulo 9 contém as propostas de encaminhamento sugeridas em função da realização deste trabalho.

1.6. Limitações ocorridas

22.Uma primeira limitação deveu-se ao prazo relativamente curto que os gestores tiveram para responder o questionário da auditoria, cuja previsão inicial era que ficasse disponível por apenas duas semanas, de 26/10 a 6/11/2020[xi]. Nessa última semana, devido aos ataques cibernéticos cuja prevenção e resposta passaram a ser prioritárias para as equipes de SegInfo das organizações públicas (Capítulo 6), esse prazo foi estendido (apenas para as organizações que ainda não haviam respondido).

23.Paralelamente ao prazo curto, devido a questões burocráticas, em algumas organizações o ofício de comunicação da auditoria enviado pelo TCU demorou mais tempo a provocar o efeito pretendido (indicação, internamente, do gestor responsável por responder o questionário). Sopesadas tais ocorrências, do universo de 422 organizações elegidas para figurarem no rol de auditadas (e para as quais, consequentemente, foram encaminhados esses ofícios), um número significativo (410, ou 97,2%) efetivamente respondeu o questionário. A evolução temporal das respostas pode ser vista na Figura 1.

24.Conforme explicitado no próprio questionário, as organizações que não o responderam, mesmo após a concessão de extensão do prazo, além de não receberem os relatórios de *feedback* (Capítulo

4), poderão, a critério da Sefti, ser selecionadas para auditorias *in loco* com vistas à verificação dos subcontroles avaliados nesta auditoria, entre outros.

25.Adicionalmente, é possível que os gestores de algumas das organizações diretamente afetadas pelos citados ataques cibernéticos tenham respondido o questionário com excessiva pressa, o que, teoricamente, poderia comprometer a qualidade das respectivas respostas. Contudo, tendo em vista o caráter prioritariamente didático dessa auditoria, esse não é um fator que gere preocupação.

26.Relativamente à qualidade das respostas recebidas por meio do questionário da auditoria, frise-se que nenhuma das organizações participantes recebeu visita *in loco* e, portanto, tais respostas são de inteira responsabilidade dos gestores respondentes. Apesar de a solicitação de evidências comprobatórias mitigar o risco de envio de respostas que não condizem com a realidade da organização (parágrafo 13), é preciso ter em mente que esse risco não é eliminado por completo. Em todo caso, como se trata de auditoria de autoavaliação (parágrafos 11-12), cabe ao gestor ter a maturidade de perceber que, numa resposta eventualmente superavaliada, a única pessoa que ele "enganou" foi a si mesmo.

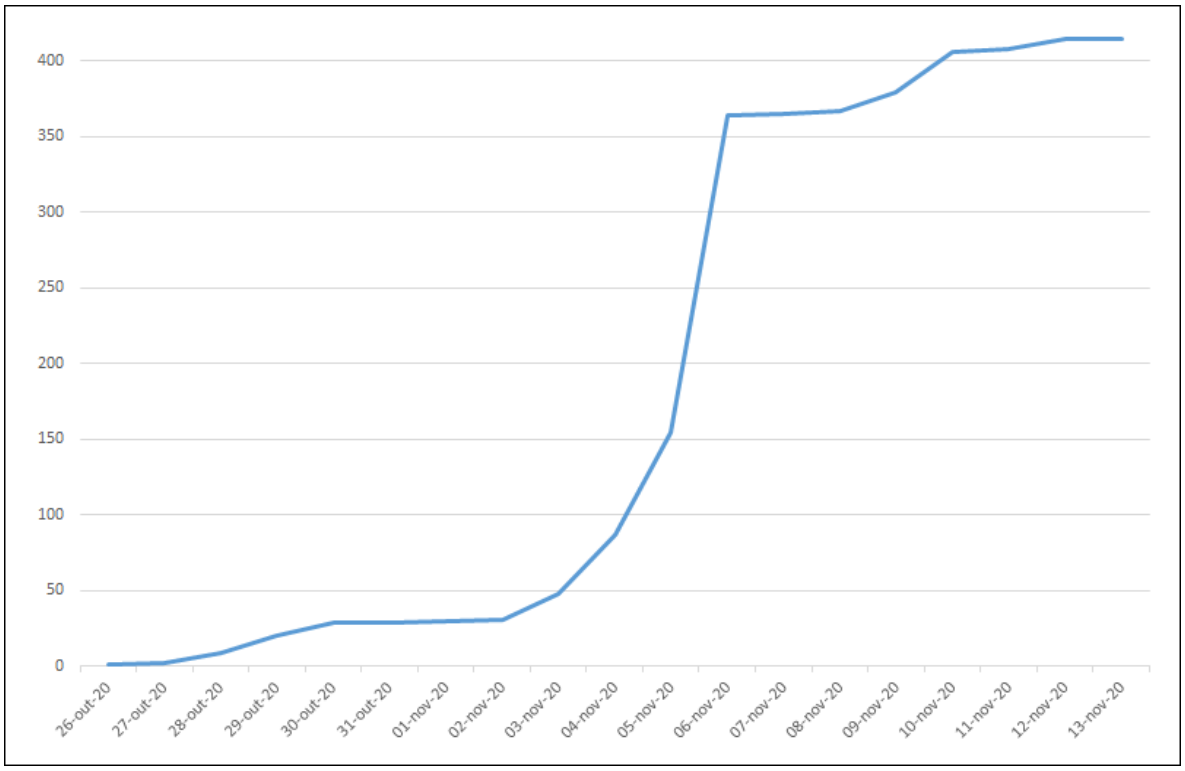


**Figura 1 - Evolução temporal das respostas ao questionário da auditoria.**
(Fonte: elaboração própria, com base nas datas de submissão dos questionários obtidas a partir da ferramenta LimeSurvey)

27.Por fim, registra-se que alguns dos auditores participantes não possuíam formação específica na área de TI. Para que esse fato não representasse limitação da auditoria, foram construídos mecanismos que permitiram a padronização das análises efetuadas, a exemplo da avaliação qualitativa de documentos por meio da utilização de *checklists* (Anexo IV - *Checklists* para verificação de política e plano de *backup*) e da elaboração dos relatórios de *feedback* a partir de modelos (*templates*) pré-concebidos. Ademais, antes da fase de execução, nos dias 21, 22 e 23/10/2020, os auditores da equipe receberam treinamentos para nivelamento de conhecimentos em vários dos aspectos a serem abordados (peça 896).

1.7. Visão geral do objeto

28.Esta auditoria foi elaborada para verificar a capacidade das organizações da APF quanto à execução de procedimentos de cópias de segurança (*backups*) e de recuperação de dados (*restore*), em especial sobre suas principais bases de dados e sistemas críticos, além de conscientizar e

orientar os respectivos gestores em relação aos riscos associados à ausência/deficiência de controles nessas áreas.

29.A "Auditoria sobre *backup*", como acabou sendo chamada, foi planejada tomando por base uma livre adaptação, a partir do julgamento profissional da equipe de auditores do TCU, dos subcontroles constituintes do décimo controle crítico de SegCiber (*Data Recovery Capabilities*) da versão 7.1 do *framework* desenvolvido pelo CIS, o qual é composto por vinte controles[xii] (Tabela 1).

**Tabela 1 - Controles críticos de SegCiber do *Center for Internet Security* (CIS).**
(Fonte: https://www.cisecurity.org/controls/cis-controls-list)

| | | |
|---|---|---|
| **Básicos** | 1 | Inventário e controle de ativos de hardware |
| | 2 | Inventário e controle de ativos de software |
| | 3 | Gerenciamento contínuo de vulnerabilidades |
| | 4 | Uso controlado de privilégios administrativos |
| | 5 | Configuração segura de hardware e software em dispositivos móveis, laptops, estações de trabalho e servidores |
| | 6 | Manutenção, monitoramento e análise de *logs* de auditoria |
| **Fundamentais** | 7 | Proteções de *e-mail* e navegador da *web* |
| | 8 | Defesas contra *malware* |
| | 9 | Limitação e controle de portas, protocolos e serviços de rede |
| | **10** | **Capacidades de recuperação de dados** |
| | 11 | Configuração segura de dispositivos de rede (*firewalls*, roteadores, *switches* etc.) |
| | 12 | Defesa de perímetro |
| | 13 | Proteção de dados |
| | 14 | Controle de acesso com base na necessidade de saber (*need to know*) |
| | 15 | Controle de acesso sem fio (*wireless*) |
| | 16 | Monitoramento e controle de contas de usuário |
| **Organizacionais** | 17 | Programa de conscientização e treinamento em segurança |
| | 18 | Segurança de aplicações de software |
| | 19 | Resposta e gerenciamento de incidentes |
| | 20 | Testes de penetração e exercícios de ataque (*red team exercises*) |

30.No *framework* do CIS, esse controle 10 ("Capacidades de recuperação de dados", em português) é subdividido em cinco subcontroles (Tabela 2). Cada um desses subcontroles se refere a uma capacidade diferente relacionada a procedimentos e rotinas de *backup*/*restore* que uma organização, idealmente, deve manter.

**Tabela 2 - Subcontroles do controle 10 (*Data Recovery Capabilities*) do *framework* do CIS.**
(Fonte: CIS Controls® Version 7.1, disponível em https://learn.cisecurity.org/cis-controls-download)

| Subcontrole | Descrição |
|---|---|

| | |
|---|---|
| 10.1 | Realize cópias de segurança (*backups*) de todos os dados da organização, de forma regular e automática |
| 10.2 | Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade |
| 10.3 | Realize, periodicamente, testes de restauração (*restore*) das cópias de segurança (*backups*) da organização, de modo a atestar seu funcionamento em caso de necessidade |
| 10.4 | Proteja adequadamente as cópias de segurança (*backups*) da organização, por meio de mecanismos de controle de acesso físico e lógico |
| 10.5 | Armazene as cópias de segurança (*backups*) da organização em ao menos um destino não acessível remotamente |

31.A metodologia utilizada na auditoria foi a autoavaliação de controles internos (CSA), tendo sido disponibilizado questionário, o qual foi respondido pelos gestores de modo a refletir os controles de *backup*/*restore* implementados nas suas respectivas organizações, anexando-se as evidências correspondentes (Seção 1.5 - Métodos utilizados).

**2. Estruturação da auditoria**

32.A auditoria foi estruturada na forma de questionário *online* (Anexo I - Questionário da Auditoria sobre *backup*), disponibilizado para preenchimento pelos gestores das organizações auditadas e composto de uma sequência de abas, cada uma com perguntas relacionadas entre si, construídas a partir das cinco macroquestões definidas na fase de planejamento (Anexo II - Planejamento da fiscalização).

33.Cada uma das seções deste capítulo corresponde a uma das diferentes abas do questionário e traz os resultados gerais das organizações em relação às perguntas nela inseridas. Nas Seções 2.2 a 2.6, portanto, encontra-se o panorama das organizações em termos dos cinco subcontroles específicos avaliados, além de, quando pertinente, alguns comentários a respeito.

34.Ao final, as respostas fornecidas pelas organizações auditadas que responderam o questionário, tomadas em conjunto, foram sintetizadas no Anexo V - Matriz de achados.

2.1. Porte da organização e política de *backup*

35.O questionário possuía uma parte inicial com algumas perguntas gerais acerca das organizações auditadas, de modo que, posteriormente, essas informações pudessem ser levadas em conta para fins de análise das respectivas respostas.

36.Para esse fim, foram questionadas, por exemplo, as quantidades de colaboradores total (Figura 2) e que atuam no setor de TI da organização (Figura 3).


**Figura 2 - Quantidade total de colaboradores da organização.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

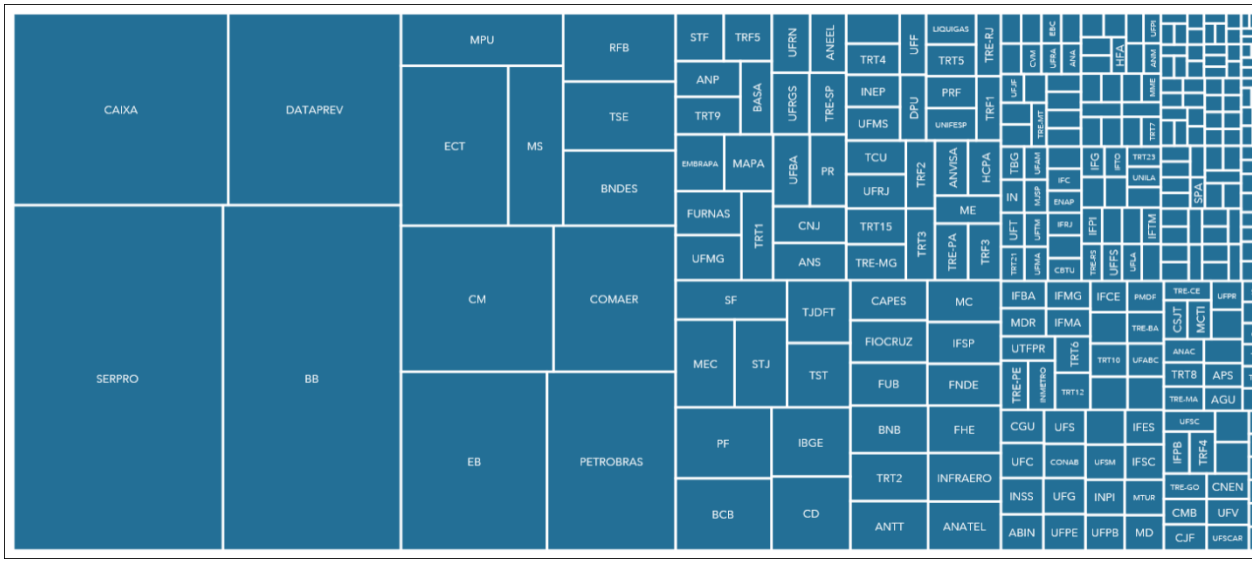


**Figura 3 - Quantidade de colaboradores do setor de TI da organização.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

37.Adicionalmente, foi questionado se a organização possuía política de *backup* ou instrumento normativo equivalente. Em linhas gerais, essa política consiste num acordo de alto nível entre as áreas de negócio ("dona" dos dados e/ou sistemas) e de TI da organização para documentar de quais dados serão feitos os *backups*, as suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança. Esses requisitos podem variar de acordo com cada base de dados ou sistema da organização, sendo que, para as bases de dados/arquivos/sistemas/aplicativos/servidores mais críticos, eles podem ser detalhados em documentos específicos, chamados planos (ou procedimentos/roteiros/*scripts*) de *backup*.

**Achado 1 - Inexistência de política de geração de cópias de segurança (*backup* e *restore*) aprovada formalmente na organização**

Situação encontrada

38.Apesar do seu caráter eminentemente básico, destaca-se que cerca de metade das organizações respondentes (208 de 410: 50,7%) ainda não possuem tal documento e, das 202 que o elaboraram, quase metade (98 de 202: 48,5%) não providenciaram a sua aprovação formal (Figura 4).

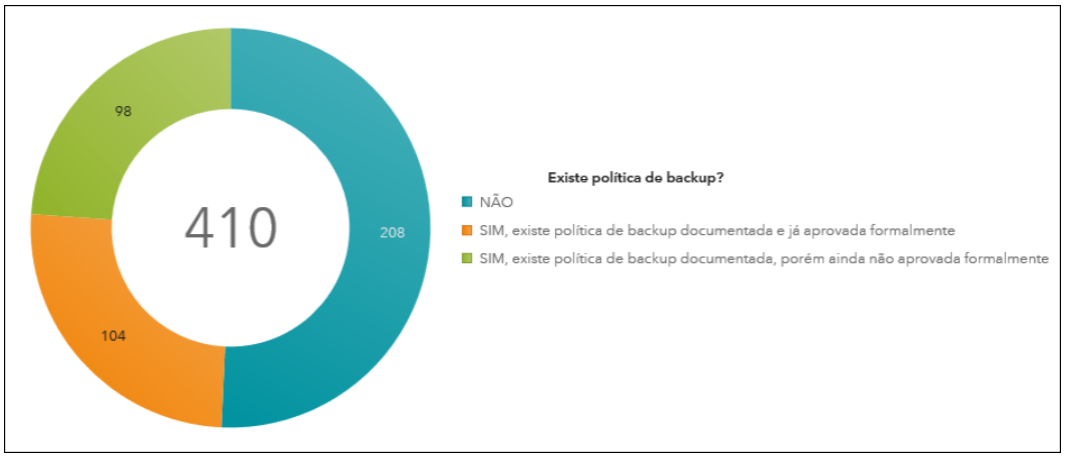


**Figura 4 - A organização possui política de *backup*?**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

Critério

39.O item 12.3 (Cópias de segurança) da norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação) prescreve que "cópias de segurança das informações, dos *software* e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida" (grifo nosso). As diretrizes para implementação desse item detalham aspectos relativos à política de *backup*.

40.Igualmente, o objetivo APO 14.10 (*Manage data backup and restore arrangements*) do *framework* Cobit 2019 prevê o estabelecimento dos requisitos relativos à realização das cópias, alinhados aos requisitos do negócio, bem como das definições das janelas de execução dos *backups* e dos testes de restauração (*restore*), além de preceituar a elaboração da política de *backup* e do respectivo plano de testes como insumos para o objetivo de governança DSS 4.07 (*Manage backup arrangements*).

Efeitos

41.A inexistência de política de *backup*, de modo geral, leva à indefinição ou à despadronização em relação ao escopo dos dados (bases de dados, sistemas de arquivos, imagens de servidores etc.) que deverão ser copiados, bem como suas respectivas periodicidades (diária, semanal, mensal etc.), tipos (completo/*full*, diferencial, incremental), quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos específicos de segurança em função dos dados copiados (controle de acesso, localização remota, criptografia etc.).

Boas práticas

42.Além de elaborada e aprovada formalmente, a política de *backup* deve ser periodicamente revisada e atualizada, de modo a se manter sempre alinhada aos requisitos do negócio, bem como para que leve em consideração a evolução das tecnologias e das soluções nessa área, que ocorre rapidamente.

Benefícios esperados

43.A partir da formalização da política de *backup* e da implementação das suas prescrições, a organização estará menos sujeita aos efeitos danosos de incidentes e/ou falhas que resultem em perda de dados, evitando, assim, prejuízos e paradas desnecessárias. Consequentemente, aumenta-se sua resiliência quanto a incidentes de SegInfo e ataques cibernéticos.

2.2. Subcontrole 1: Realize cópias de segurança (*backups*) de todos os dados da organização, de forma regular e automática

44.De maneira bem direta, esse primeiro subcontrole se refere à capacidade de a organização realizar e armazenar cópias de segurança (*backups*) de todos os seus dados. Quando se fala em

continuidade do negócio, a implementação de tal subcontrole é crucial, pois permite que a organização tenha condições de se recuperar de incidentes que resultem no comprometimento, mesmo que parcial, dos seus dados, a exemplo de uma falha de software/hardware, um desastre natural ou mesmo a disseminação de um software nocivo (*malware*) ou um ataque cibernético.

45.Lembrando que, no atual contexto de transformação digital da Administração Pública, praticamente todas as informações relevantes das organizações já são tratadas em formato eletrônico, muitas vezes sem possuir correspondência alguma no mundo físico (documentos e/ou processos em papel, por exemplo). Assim, qualquer perda de dados que, eventualmente, não possam ser recuperados, tem o potencial de acarretar enormes prejuízos, pois pode afetar ou mesmo inviabilizar os processos de negócio do órgão em questão, bem como a prestação de serviços públicos para a sociedade.

46.Justamente com o objetivo de explorar essa vulnerabilidade, há os ataques de *ransomware*, realizados por meio de *malwares* programados para "sequestrar" dados e cobrar um "resgate", via de regra em criptomoedas. Esse "sequestro", geralmente, ocorre bloqueando o acesso ao conteúdo dos arquivos de dados criptografando-os com a utilização de uma chave muito difícil de ser quebrada, a qual só é fornecida à vítima, para o respectivo desbloqueio, mediante o pagamento do referido "resgate"[xiii].

47.Para se ter ideia do risco ao qual as organizações estão expostas, basta constatar que, segundo dados da empresa Kaspersky, o Brasil "lidera a lista dos países mais afetados por ataques de *ransomware* empresariais ao redor do mundo"[xiv], sendo, atualmente, "alvo de quase metade dos ataques de *ransomware* na América Latina"[xv].

48.A partir, então, da realização de cópias de segurança (*backups*) dos seus dados, a organização passa a ter a possibilidade de recuperá-los em caso de perda/comprometimento, seja em virtude de ataques cibernéticos ou de falhas e incidentes em geral, os quais podem, inclusive, ter causas naturais, como incêndios, relâmpagos, enchentes etc.

49.Frise-se que, a fim de realizar tal verificação, esta auditoria questionou tão somente a execução de cópias de segurança (*backups*) em relação à principal base de dados tratada "diretamente" pela organização auditada, ou seja, cuja custódia e tratamento dos respectivos dados são de sua inteira responsabilidade, não de algum órgão vinculador.

Questões 1.1, 1.2 e 1.3

50.Essas questões objetivaram filtrar as organizações que mantém bases de dados próprias (Questão 1.1), identificar essas bases (Questão 1.2) e dimensionar seu tamanho aproximado, em megabytes – MB (Questão 1.3).

Questão 1.4

51.Essa questão pretendeu identificar as principais ferramentas utilizadas pelas organizações públicas para gerenciar os *backups* das suas bases de dados. Por meio da nuvem de palavras apresentada na Figura 5, verifica-se que são utilizadas muitas ferramentas, sendo as que mais se destacam: Bacula (software livre), Veritas NetBackup, IBM Spectrum Protect, Commvault, HP Data Protector e Veeam.

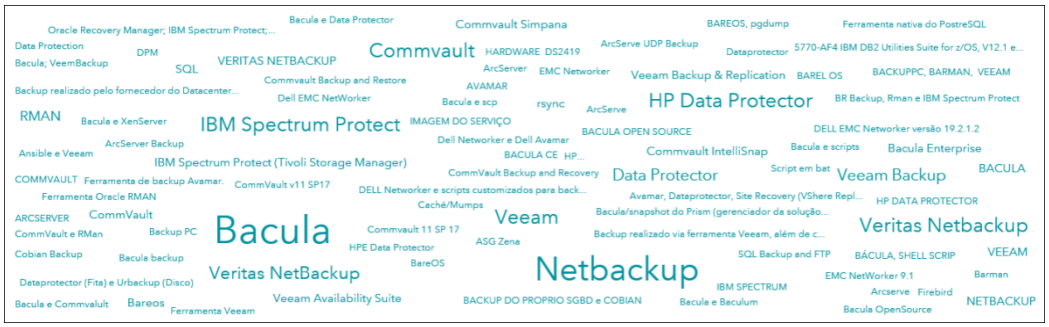


**Figura 5 - Nuvem com os tamanhos das palavras proporcionais ao número de vezes que foram citadas nas respostas fornecidas pelas organizações à pergunta 1.4 do questionário.**

(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

Questão 1.5

52.Essa questão buscou verificar a periodicidade com a qual as organizações realizam *backups* completos (*full*), diferenciais e incrementais das suas principais bases de dados.

53.O *backup full*, que serve de referência para os outros dois tipos, consiste na execução de uma cópia completa (replicação) dos arquivos, pastas ou volumes em questão para outro destino, que pode ser um sistema de discos ou fitas próprias para *backup*, do tipo *Linear Tape-Open* (LTO), um servidor ou mesmo outro tipo de mídia (DVD, CD, *pendrive* etc.). No *backup* diferencial, são copiados todos os dados alterados desde o último *backup full*. No incremental, a seu turno, são copiados apenas os dados alterados desde o último *backup* realizado, seja ele *full*, diferencial ou incremental (Figura 6)[xvi].

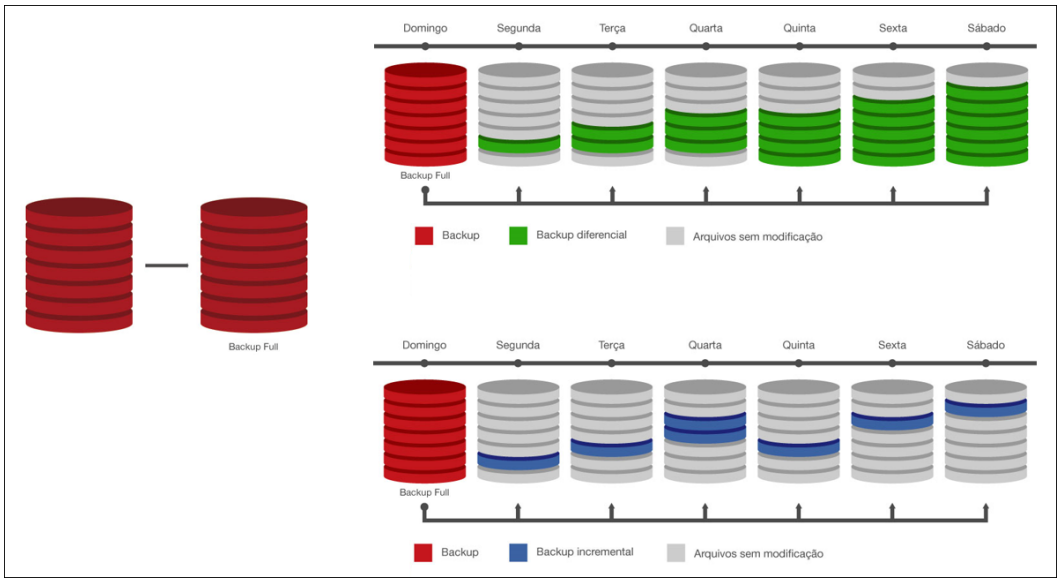


**Figura 6 - Tipos de *backup* (completo/*full*, diferencial e incremental).**
(Fonte: https://www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial)

54.Percebe-se que o *backup full*, apesar da sua lógica de realização mais simples, demanda mais recursos (tempo, processamento, tráfego de rede e espaço de armazenamento) para ser executado. Quanto maior for a quantidade dos dados envolvidos, mais demorada será tanto a realização do *backup* em si quanto sua eventual restauração (*restore*), em caso de necessidade. Por outro lado, os *backups* diferencial e incremental exigem menos recursos a cada execução, pois apenas parte dos dados é copiada.

55.Assim, o recomendado é alternar a realização de cópias completas com a execução de *backups* diferenciais e/ou incrementais em periodicidades adequadas às necessidades específicas de cada negócio, as quais devem ser previamente definidas por meio da política e dos planos de *backup*, de acordo com a frequência com que os dados em questão são criados e modificados.

56.Com isso, uma organização com grau de maturidade mais elevado tende a definir e a manter um leque de *backups* de tipos variados, sempre levando em consideração as particularidades do seu negócio, o seu apetite a riscos, os custos associados e, principalmente, o *trade-off* (“perdas-e-ganhos”) entre a performance na execução das cópias e a prontidão de sua eventual restauração. Ela pode, por exemplo, executar um *backup* completo semanalmente, com *backups* incrementais diários.

Questão 1.6

57.Essa questão procurou identificar a forma de realização dos *backups* completos da principal base de dados da organização, podendo ser manual (algum funcionário precisa dar o comando para

a execução do *backup*), automatizada (o *backup* ocorre regularmente, de forma automática, de acordo com a periodicidade definida na ferramenta de gerenciamento) ou, ainda, feita de outra maneira (a ser descrita pelo respondente em campo próprio, caso não se enquadrasse em nenhuma das opções anteriores).

**Achado 2 - Cópias de segurança (*backups*) da principal base de dados da organização são realizadas de forma regular e automática [ACHADO POSITIVO]**

Situação encontrada

58.No que tange à regularidade de realização dos *backups* das suas principais bases de dados (Questão 1.5), percebe-se que 99,2% (373 de 376) das organizações que afirmaram tratar diretamente alguma base de dados executam *backups* completos dessa base com alguma periodicidade (Tabela 3). Dessas, inclusive, 45,9% (171 de 373) o fazem diariamente ou mais de uma vez por dia.

**Tabela 3 - Periodicidade dos *backups* da principal base de dados das organizações.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

| **Periodicidade do *backup*** | **Tipo do *backup*** | | |
|---|---|---|---|
| | **Completo (*full*)** | **Diferencial** | **Incremental** |
| Não são realizados | 3 | 238 | 129 |
| Ocasionalmente (menos do que uma vez por mês) | 9 | 4 | 5 |
| Mensalmente | 55 | 5 | 2 |
| Semanalmente | 138 | 26 | 8 |
| Diariamente | 138 | 61 | 148 |
| Mais de uma vez por dia | 33 | 42 | 84 |
| **TOTAL** | **376** | **376** | **376** |

59.Um plano de *backup* deve ser definido com base no volume de dados e na frequência de atualização. De modo geral, utiliza-se uma combinação da execução de *backups* completos e de *backups* diferenciais e/ou incrementais.

60.Um esquema bastante comum é a realização de *backups full* semanais e incrementais diários. Essa sistemática é sugerida no fascículo relativo a *backup* da Cartilha de Segurança para Internet do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br)[xvii]. De fato, uma verificação mais aprofundada das respostas ao questionário mostrou que, das 138 organizações que afirmaram realizar *backups* completos semanalmente, 108 também sinalizaram executar *backups* incrementais diariamente ou mais de uma vez por dia. E, dessas mesmas 138 organizações, 46 disseram fazer *backups* diferenciais diariamente ou mais de uma vez por dia.

61.Seguindo esse mesmo raciocínio, caso a frequência de atualização dos dados não seja grande, outro esquema que pode ser adotado é a realização de *backups full* mensais e incrementais diários. No caso das 55 organizações que responderam fazer cópias completas mensalmente, por exemplo, essa análise mostrou que 44 também fazem *backups* incrementais diariamente ou mais de uma vez por dia.

62.A seu turno, quanto à forma de execução dos *backups* completos da principal base de dados (Questão 1.6), tem-se que a grande maioria (354 de 373: 94,9%) é automatizada (Figura 7), isto é, ocorrem sem que um colaborador precise, pessoalmente, executar algum comando.

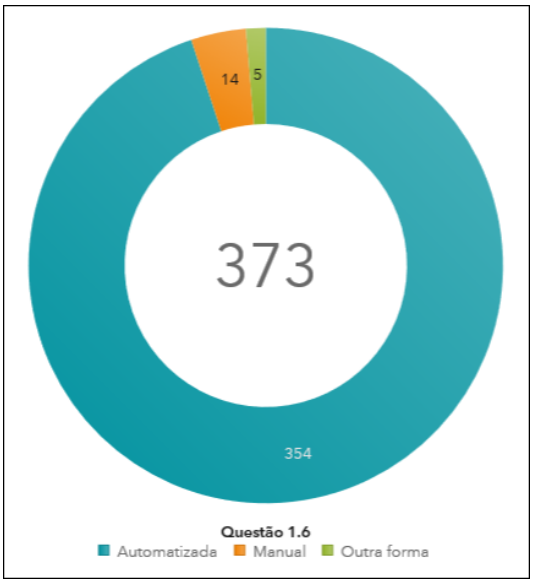


**Figura 7 - Forma de realização dos *backups* completos (*full*) da principal base de dados.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

Critério

63.*Framework* de controles críticos de SegCiber do CIS, controle 10 (*Data Recovery Capabilities*), subcontrole 10.1 – *Ensure Regular Automated Backups* (Tabela 2).

Benefícios esperados

64.A execução periódica dos *backups* diminui o risco de perda de dados, tendo em vista que, na ocorrência de qualquer evento que possa ter essa consequência, basta que a organização recupere os dados em questão a partir das respectivas cópias. Também por isso, é desejável que a frequência de realização dos *backups* seja a maior possível, pois, assim, diminui-se a janela de dados efetivamente sujeitos a perda (aqueles que sofreram alteração desde o último *backup* disponível).

65.Por sua vez, a forma de execução automatizada é recomendada, pois, ao contrário de procedimentos manuais, previne esquecimentos e erros de execução.

2.3. Subcontrole 2: Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade

66.Conforme visto no subcontrole anterior, há três tipos principais de *backup* (completo/*full*, diferencial e incremental), cada um com vantagens e desvantagens, sobretudo no que se refere à rapidez com que os dados podem ser obtidos e restaurados, em caso de necessidade (parágrafos 53-54).

67.Relativamente a seus sistemas críticos, no entanto, convém que a organização execute *backups* integrais (cópia/espelhamento da imagem dos servidores/máquinas envolvidos) com alguma periodicidade, de modo que, em caso de necessidade, possa recuperar tais sistemas em curto espaço de tempo, visto que, a depender da criticidade do sistema, sua parada pode interromper/inviabilizar o próprio negócio da organização.

68.Para realizar a verificação deste subcontrole, a auditoria perguntou sobre a execução de cópias de segurança (*backups*) integrais do servidor ou conjunto de servidores/máquinas que hospedam o principal sistema da organização auditada, isto é, cuja gestão não está sob a responsabilidade de algum órgão vinculador, mas, sim, da própria organização, que fica responsável pela manutenção, evolução e gerência do referido sistema.

Questões 2.1 e 2.2

69.Essas questões pretenderam filtrar as organizações que mantém sistemas em servidor ou conjunto de servidores/máquinas próprios (2.1) e identificar tais sistemas (2.2).

Questão 2.3

70.Essa questão buscou identificar as principais ferramentas utilizadas pelas organizações públicas para gerenciar os *backups* dos seus servidores/máquinas. Assim como na Questão 1.4, por meio da nuvem de palavras, verifica-se que são utilizadas muitas ferramentas, sendo, novamente, as que mais se destacam: Veritas NetBackup, Veeam, Commvault, Bacula (software livre), HP Data Protector e IBM Spectrum Protect (Figura 8).

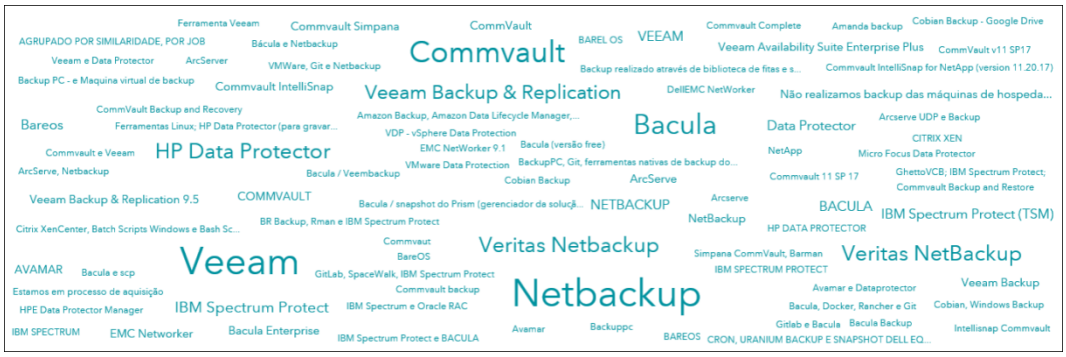


**Figura 8 - Nuvem com os tamanhos das palavras proporcionais ao número de vezes que foram citadas nas respostas fornecidas pelas organizações à pergunta 2.3 do questionário.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

Questão 2.4

71.Essa questão aferiu a periodicidade com a qual as organizações realizam *backups* dos servidores/máquinas que hospedam seu principal sistema.

Questão 2.5

72.Essa questão buscou identificar a forma de realização dos *backups* do principal sistema da organização, podendo ser parcial (cópia apenas de determinados arquivos das máquinas), integral (cópia/espelhamento da imagem das máquinas ou procedimento assemelhado) ou, ainda, feita de outra forma (a ser descrita pelo respondente, caso não se enquadrasse nas opções anteriores).

Questão 2.7

73.Esse item questionou as organizações quanto à existência ou não de plano de *backup* específico (parágrafo 37) para seu principal sistema.

**Achado 3 - Cópias de segurança (*backups*) integrais (*e.g.* cópia da imagem das máquinas) do principal sistema da organização são realizadas regularmente [ACHADO POSITIVO]**

Situação encontrada

74.No total, 372 organizações afirmaram hospedar sistemas em servidores/máquinas próprios. A Figura 9 traz as respostas quanto à periodicidade dos *backups* do seu principal sistema (Questão 2.4).

75.Percebe-se que 8,9% das organizações (33 de 372), por não realizarem *backups* do seu principal sistema, encontram-se totalmente vulneráveis a falhas e a ataques de *ransomware*. A seu turno, outras 6,7% das organizações também estão expostas a risco considerável, pois, apesar de até executarem esses *backups*, o fazem com periodicidade, possivelmente, insuficiente (mensal: 2,1% [8 de 372]; menos do que uma vez por mês: 4,6% [17 de 372]). As demais (84,4%) realizam esses *backups* semanalmente (32 de 372: 8,6%), diariamente (246 de 372: 66,1%) ou até mais de uma vez por dia (36 de 372: 9,7%).

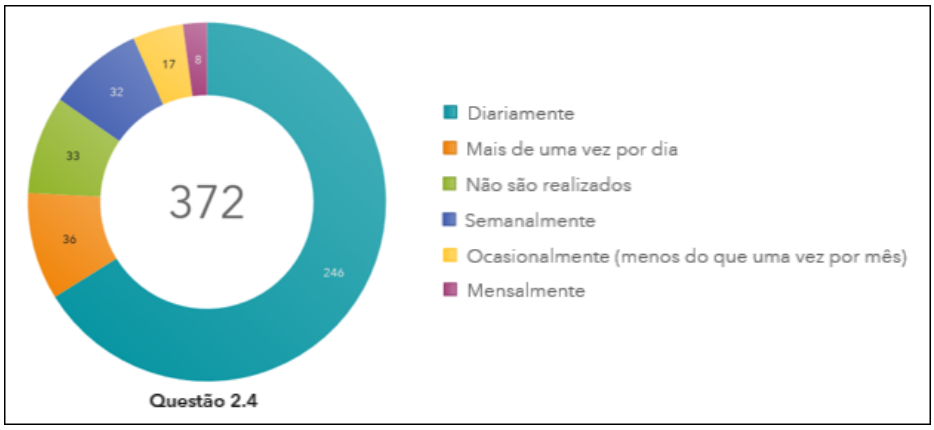


**Figura 9 - Periodicidade dos *backups* do principal sistema das organizações.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

76.Um plano de *backup* deve ser definido conforme a frequência de atualização do sistema, mas, de modo geral, intervalos menores (diariamente ou mesmo mais de uma vez por dia) entre os *backups* – assim como fazem a maioria das organizações auditadas – são recomendados para sistemas que sofrem constantes modificações e atualizações.

77.A Questão 2.5, a seu turno, mostrou que, descontadas as 33 organizações que não realizam cópias de segurança do seu principal sistema, das demais 339, a maioria (206 de 339: 60,8%) executa *backups* integrais (cópia/espelhamento da imagem dos servidores/máquinas), enquanto um quarto (84 de 339: 24,8%) faz *backups* apenas parciais (cópia de parte dos arquivos dos servidores) e 14,4% (49 de 339) realizam, ainda, alguma outra forma de *backup* (Figura 10).

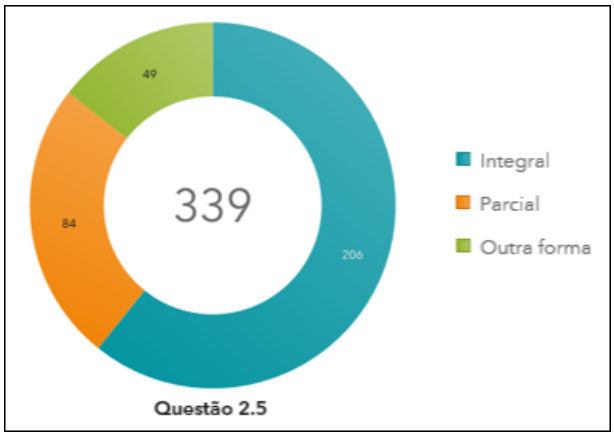


**Figura 10 - Forma de realização dos *backups* do principal sistema.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

78.Enquanto os *backups* integrais ocupam mais espaço e têm uma execução mais demorada, os parciais são mais simples, ocupam menos espaço e são realizados mais rapidamente. Além dessas diferenças, os *backups* integrais também facilitam a recuperação dos dados caso seja necessário trocar o equipamento, ao passo que os parciais tornam mais fácil a restauração de arquivos específicos.

79.Assim sendo, a escolha entre a realização de *backups* integrais e/ou parciais vai depender da análise de fatores tais como a complexidade, o tamanho e a frequência de atualização do sistema. Pode ser adotada, também, uma combinação de ambos os tipos, a exemplo do que fazem várias das organizações auditadas, as quais deixaram tal fato registrado no campo de comentário dessa questão.

Critério

80.*Framework* de controles críticos de SegCiber do CIS, controle 10 (*Data Recovery Capabilities*), subcontrole 10.2 – *Perform Complete System Backups* (Tabela 2).

Benefícios esperados

81.A realização de cópias integrais dos servidores/máquinas que hospedam o principal sistema da organização permite sua pronta e rápida recuperação em caso de necessidade (falha, ataque ou qualquer outro tipo de incidente). Além disso, também permite que o sistema seja rapidamente restaurado no caso de troca dos equipamentos (realização de *upgrades* nas máquinas, por exemplo).

**Achado 4 - Inexistência de plano de *backup* específico para o principal sistema da organização**

Situação encontrada

82.A Questão 2.7 identificou que menos de um terço das organizações que hospedam sistemas em máquinas próprias (107 de 372: 28,8%) possuem plano de *backup* específico para seu principal sistema, enquanto a grande maioria (265 de 372: 71,2%) não o elaborou. Para essas últimas, na ausência de uma avaliação focada nesse sistema, existe o risco de que, na prática, os *backups* estejam sendo realizados em desacordo com as necessidades específicas do sistema e, consequentemente, do negócio.

Critério

83.As diretrizes para implementação do item 12.3 (Cópias de segurança) da norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação) trazem aspectos importantes a serem considerados quando da elaboração dos planos de *backup*, tais como "a abrangência (por exemplo, completa ou diferencial) e a frequência da geração das cópias de segurança (...), além dos requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização", o armazenamento das cópias em localidade remota, a "proteção física e ambiental das informações das cópias" e a necessidade de uso da encriptação para proteger a confidencialidade das informações.

84.O objetivo de governança APO 14.10 (*Manage data backup and restore arrangements*) do *framework* Cobit 2019 também prevê, entre suas atividades, a definição de requisitos relacionados ao volume dos dados a serem copiados, à capacidade de armazenamento e ao período de retenção das cópias, de acordo com os requisitos do negócio.

Efeitos

85.A inexistência de plano de *backup* acarreta indefinição ou despadronização em relação ao escopo dos dados que deverão ser copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança.

Boas práticas

86.Além de elaborado e aprovado formalmente, o plano de *backup* deve ser revisado e atualizado periodicamente, de modo a se manter alinhado aos requisitos do negócio e levar sempre em consideração as constantes evoluções tecnológicas verificadas nessa área.

Benefícios esperados

87.A formalização do plano de *backup* atua para diminuir o risco de que o principal sistema da organização venha a sofrer qualquer descontinuidade, evitando prejuízos e aumentando sua resiliência em relação a incidentes de SegInfo e ataques cibernéticos.

2.4. Subcontrole 3: Realize, periodicamente, testes de restauração (*restore*) das cópias de segurança (*backups*) da organização, de modo a atestar seu funcionamento em caso de necessidade

88.A partir dos subcontroles anteriores, assegura-se que a organização realize *backups* tanto dos seus dados (subcontrole 1) quanto dos seus sistemas críticos (subcontrole 2). Tendo em vista que os processos de trabalho das organizações, atualmente, dependem intrinsecamente de sistemas e de bases de dados, percebe-se que tais subcontroles são, realmente, essenciais para a continuidade do negócio.

89.No entanto, de nada adianta realizar esses *backups* se eles não puderem ser restaurados sem problemas quando preciso. Essa é, justamente, a função do terceiro subcontrole do *framework* do CIS, o qual preconiza a realização periódica de testes de restauração (*restore*) sobre esses *backups*, de modo a atestar que, sempre que efetivamente necessário, a recuperação dos sistemas e/ou dos dados da organização a partir das cópias de segurança armazenadas irá funcionar perfeitamente.

90.Além de garantir seu funcionamento em situações reais nas quais seja necessário restaurar algum *backup*, esses testes periódicos permitem que os gestores tenham maior clareza acerca dos custos associados à manutenção de controles efetivos de *backup*/*restore* e, com isso, percebam que, em geral, implementar esses controles na organização pode custar significativamente menos do que os prejuízos decorrentes de eventuais falhas ou do pagamento do valor exigido por um criminoso a título de "resgate" dos dados (sob pena de parar o negócio da organização, por exemplo), em eventual caso de *ransomware*.

91.Para realizar a verificação deste subcontrole, a auditoria perguntou sobre a execução do procedimento de restauração (*restore*) em relação aos *backups* da principal base de dados e dos servidores/máquinas que hospedam o principal sistema da organização auditada.

Questão 3.1

92.Essa pergunta questionou se a organização executa, periodicamente, testes de restauração (*restore*) sobre os seus *backups*.

Questão 3.2

93.Esse item perguntou, basicamente, se os testes de restauração (*restore*) são documentados, ou seja, se geram algum tipo de registro ou relatório de resultados.

Questão 3.4

94.Essa questão levantou a periodicidade de realização dos testes de restauração (*restore*) dos *backups* das principais bases de dados e dos principais sistemas das organizações (Tabela 4).

**Tabela 4 - Periodicidade dos testes de restauração (*restore*) dos *backups*.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

| **Periodicidade do teste de restauração (*restore*) do *backup*** | **Da principal base de dados** | **Dos servidores/máquinas do principal sistema** |
|---|---|---|
| Não são realizados | 11 | 11 |
| Ocasionalmente (menos do que uma vez a cada três meses) | 71 | 46 |
| A cada três meses | 20 | 17 |
| Mensalmente | 32 | 16 |
| Semanalmente | 18 | 7 |
| Diariamente | 24 | 6 |
| **TOTAL** | **176** | **103** |

95.Nota-se que, das 176 (91 + 85) organizações que, na Questão 3.1, afirmaram executar esses testes em relação aos *backups* da principal base de dados (parágrafo 97), 11 responderam nesta questão que, na verdade, não o fazem. Das que efetivamente realizam esses testes, mais da metade (91 de 165: 55,2%) o faz esporadicamente (a cada três meses, ou nem isso), enquanto apenas as demais (74 de 165: 44,8%) executam esses testes de restauração com certa frequência (mensal, semanal ou diariamente).

96.Em relação aos *backups* dos servidores/máquinas que hospedam o principal sistema, das 103 (18 + 85) organizações que, na Questão 3.1, declararam realizar testes de restauração (parágrafo 97), 11 também responderam nesta questão que, na verdade, não os executam. Das que efetivamente conduzem esses testes, mais de dois terços (63 de 92: 68,5%) o faz esporadicamente (a cada três meses, ou menos), ao passo que somente o restante (29 de 92: 31,5%) realiza esses testes ao menos uma vez por mês.

**Achado 5 - A organização não realiza ou não documenta os testes de restauração (*restore*) das suas cópias de segurança (*backups*)**

Situação encontrada

97.A Questão 3.1 identificou que, das organizações respondentes, mais da metade (216 de 410: 52,7%) não realiza testes de restauração (*restore*) dos *backups*. Das que realizam esses testes, quase metade (91 de 194: 46,9%) o faz somente em relação aos *backups* da sua principal base de dados, 9,3% (18 de 194) apenas em relação aos *backups* dos servidores/máquinas que hospedam seu principal sistema e 43,8% (85 de 194) os executam em relação a ambos (Figura 11).

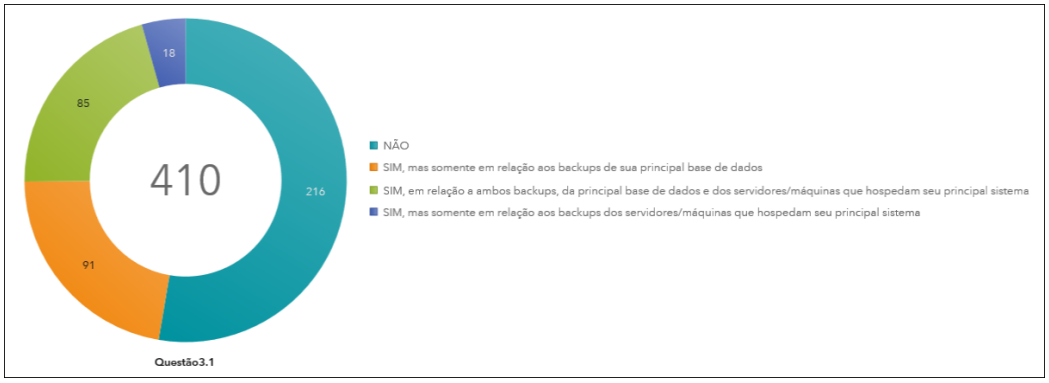


**Figura 11 - A organização executa, periodicamente, testes de restauração (*restore*) dos seus *backups*?**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

98.Por sua vez, a Questão 3.2 identificou que, das 194 organizações que afirmaram realizar esses testes, a maioria (116 de 194: 59,8%) não os documenta.

Critério

99. *Framework* de controles críticos de SegCiber do CIS, controle 10 (*Data Recovery Capabilities*), subcontrole 10.3 – *Test Data on Backup Media* (Tabela 2).

Efeitos

100. As organizações que não testam a restauração das suas cópias de segurança ou que, então, realizam esses testes de forma excessivamente esporádica, encontram-se expostas a significativo risco, visto que eventuais falhas nos arquivos dos *backups* ou mesmo nas mídias utilizadas para guardá-los podem passar desapercebidas e, quando necessário, acabarem por inviabilizar a recuperação dos dados e/ou sistemas. Conforme apontado em relatório recente, o qual pesquisou mais de três mil tomadores de decisões em empresas globais, essa situação, aliás, é a regra, com 58% dos *backups* realizados apresentando falhas e, consequentemente, deixando os dados desprotegidos[xviii].

101. Igualmente, essas organizações podem ser surpreendidas negativamente por manterem rotinas de *backup* mal configuradas (com periodicidade inadequada e sem o escopo completo dos dados necessários, por exemplo), pela inexecução ou execução defeituosa dessas rotinas e/ou mesmo pelo eventual corrompimento das mídias utilizadas para armazenar os *backups*.

Boas práticas

102. Sobretudo em organizações de maior porte, pode ser inviável testar a restauração dos *backups* de todos os sistemas e bases de dados, devido à sua quantidade. Nesses casos, uma boa prática identificada é a realização de sorteios dos sistemas/bases a serem testados em cada período, em regime de rodízio, assegurando, assim, que, com alguma periodicidade, todos(as) sejam testados.

Benefícios esperados

103. A realização dos testes de restauração (*restore*) dos arquivos dos *backups* aumenta a garantia de que, em situações reais em que a organização precise recuperar algum sistema e/ou dados a partir das cópias armazenadas, essa operação seja executada com sucesso.

2.5. Subcontrole 4: Proteja adequadamente as cópias de segurança (*backups*) da organização, por meio de mecanismos de controle de acesso físico e lógico

104. Uma vez que, nos casos de *ransomware*, os profissionais de segurança das organizações mais maduras passaram a realizar procedimentos de restauração (*restore*) de *backups* ao invés de pagarem os valores solicitados pelos cibercriminosos a título de "resgate" dos dados, progressivamente os malfeitores e seus softwares maliciosos (*malwares*), como forma de impedir essa restauração, passaram a incluir, também, os próprios arquivos de *backup* entre os alvos principais dos ataques.

105. Com isso, a implementação de mecanismos de controle de acesso físico (*e.g.* ambiente segregado) e lógico (*e.g.* criptografia) relativamente aos arquivos das cópias de segurança (*backups*) tornou-se cada vez mais importante, sendo esse, justamente, o foco do quarto subcontrole do controle relativo aos procedimentos de *backup*, no *framework* do CIS.

106. Ademais, uma vez que muitos desses *backups* são armazenados em sítios remotos ou mesmo em servidores hospedados na "nuvem" (*cloud services*) e, portanto, acabam trafegando em redes de dados, é preciso que as soluções que gerenciam esses arquivos implementem controles criptográficos para garantir que eles não apenas sejam armazenados (*data at rest*) cifrados, mas, também, que não trafeguem (*data in transit*) em claro nas redes da organização ou na Internet.

107. A criptografia, aliás, atua como mecanismo de proteção adicional, tendo em vista que os malfeitores, além de cobrarem "resgate" pela devolução em si dos dados, podem tentar receber valores ameaçando publicar os dados "sequestrados", sobretudo se o incidente envolver dados sensíveis e/ou sigilosos. Nesses casos, a vítima pode, tranquilamente, recusar-se a pagar qualquer valor ao atacante, pois, além de ser plenamente capaz de restaurar seus dados a partir dos *backups*, pode confiar que os dados "sequestrados" estarão adequadamente protegidos da ameaça de vazamento devido à cifragem.

Questão 4.1

108. Essa questão procurou identificar o local de armazenamento dos arquivos dos *backups* da organização, sendo o gestor instado a responder em relação aos *backups* que considerasse melhor protegidos entre aqueles da principal base de dados e aqueles do principal sistema da organização.

109. Descartadas as 25 organizações que afirmaram não realizar *backups*, a grande maioria (342 de 385: 88,8%) guarda os arquivos na sua própria sede, sendo que algumas delas, por precaução, ainda armazenam cópias em uma localidade remota (119 de 385: 30,9%), em um serviço de hospedagem na "nuvem" (27 de 385: 7%) ou em ambos (6 de 385: 1,6%). Entretanto, 9,1% dessas organizações (35 de 385) disseram manter os arquivos somente em um sítio remoto, ao passo que 2,1% (8 de 385) os armazenam apenas na "nuvem" (Figura 12).

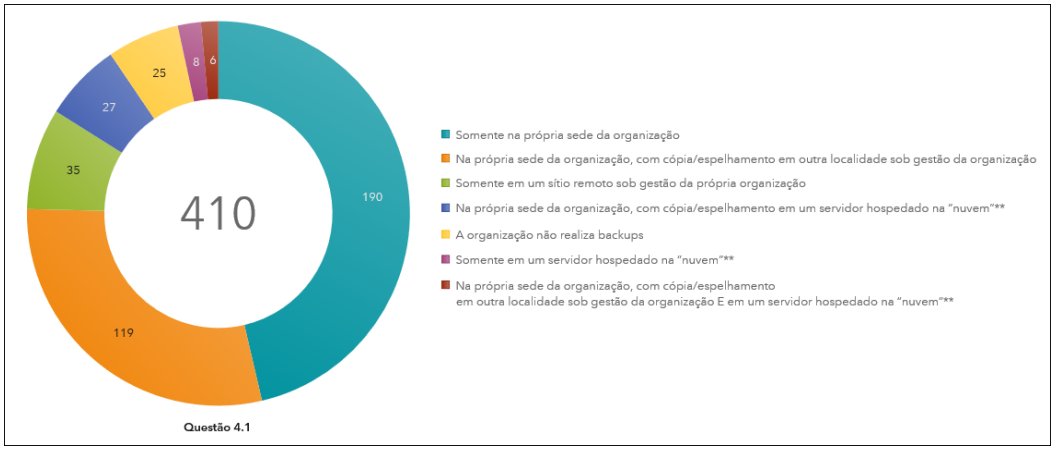


**Figura 12 - Local de armazenamento dos arquivos de *backup*.**

(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

110. Destaca-se, aqui, a situação de risco em que se encontram quase metade dessas organizações (190 de 385: 49,4%), por armazenarem os arquivos dos *backups* somente nas suas próprias sedes, visto que, em caso de acidente (*e.g.* incêndio, inundação), tanto os dados originais quanto as cópias acabarão se perdendo. Assim, recomenda-se manter, pelo menos, um *backup* local e outro remoto.

111. Cabe aqui, também, lembrar que os itens 5.3 e 5.4 da Norma Complementar (NC) 14/IN01/DSIC/GSIPR[xix] (que estabelece princípios, diretrizes e responsabilidades relacionados à SegInfo para o tratamento das informações dos órgãos e entidades da APF em ambiente de computação em nuvem) estipulam que os dados, metadados, informações e conhecimento, produzidos ou custodiados por essas organizações, bem como suas cópias de segurança, devem residir em território brasileiro.

112. A seu turno, a NC 19/IN01/DSIC/GSIPR[xx] (que estabelece padrões mínimos de SegInfo para os sistemas estruturantes da APF) traz uma série de princípios, diretrizes e procedimentos aplicáveis a tais sistemas, incluindo a obrigatoriedade de localização física nas dependências de organização da APF em território nacional (item 4.2.1) e de manutenção de sítio alternativo que garanta a disponibilidade do sistema em caso de sinistro (item 4.2.5.e).

Questões 4.2 e 4.3

113. Nos casos de manifestação de que os arquivos eram armazenados em uma localidade remota, solicitou-se o respectivo endereço (4.2). Ademais, nos casos de contratação de serviços de hospedagem em "nuvem" (*cloud services*), pediu-se a indicação da(s) empresa(s) contratada(s) (4.3).

Questão 4.4

114. Essa questão buscou identificar a aplicação de criptografia sobre as cópias de segurança.

Questão 4.5

115. Essa pergunta questionou a segurança física do ambiente próprio no qual os arquivos dos *backups* são armazenados e, portanto, também desconsiderou as 8 organizações que haviam respondido que suas cópias ficam armazenadas somente em servidores hospedados na "nuvem" (parágrafo 109).

116. Das 377 restantes, 35,8% (135 de 377) disseram guardar esses arquivos em ambientes segregados com controle mecânico e a maioria (213 de 377: 56,5%) afirmou mantê-los em ambientes dotados de controle eletrônico de acesso, enquanto apenas 7,7% (29 de 377) indicaram que o local de armazenamento não possui nenhum mecanismo de controle de acesso físico (Figura 13).

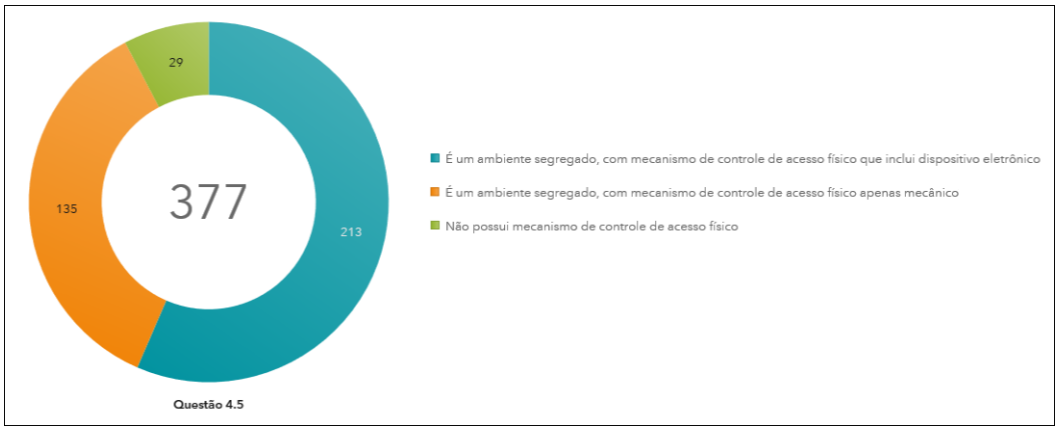


**Figura 13 - Controle de acesso físico no local de armazenamento dos arquivos de *backup*.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

117. Ao contrário dos mecanismos puramente mecânicos (*e.g.* porta com chave), os dispositivos eletrônicos permitem implementar controles adicionais (*e.g.* permissão de acesso com base no dia da semana/horário, no perfil concedido ao usuário ou mesmo em suas características biométricas) e automatizar o processo de geração e guarda dos registros (*logs*) de acesso ao ambiente.

118. Convém lembrar, também, que a NC 19/IN01/DSIC/GSIPR[24] prevê a implementação de mecanismos de proteção física nos sistemas estruturantes da APF (item 4.2.5.a).

Questão 4.6

119. Entre as 348 organizações que manifestaram possuir controles de acesso físico ao ambiente de armazenamento das cópias de segurança, questionou-se o tipo específico de mecanismo, podendo ser algo que somente o usuário sabe (*e.g.* senha), possui (*e.g.* cartão de acesso), é (*e.g.* características biométricas) ou mesmo uma combinação desses fatores, que é a opção mais recomendada e segura. Os resultados encontram-se na Figura 14.

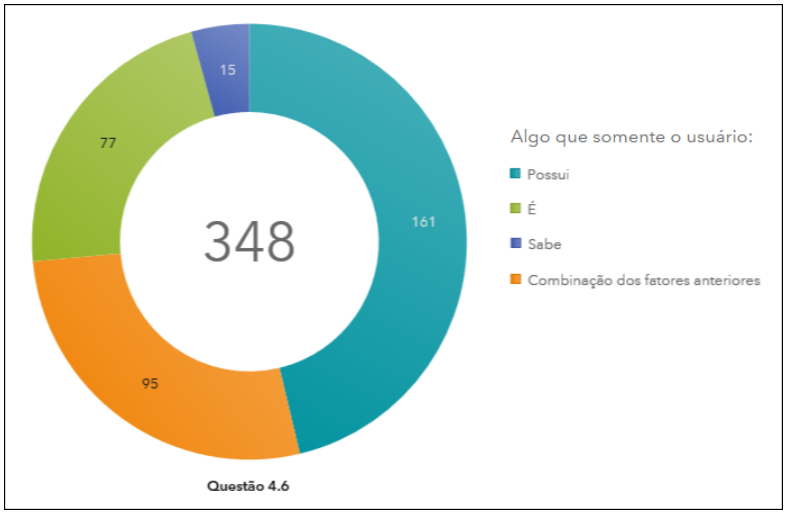


**Figura 14 - Mecanismo de concessão da permissão de acesso ao ambiente segregado.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

Questão 4.8

120. Essa pergunta questionou se os acessos ao ambiente segregado são registrados, isto é, se são guardados *logs* desses acessos, contendo identificador, data/hora e nome de quem realizou o acesso.

**Achado 6 - A organização não protege adequadamente suas cópias de segurança (*backups*)**

Situação encontrada

121. Por meio da Questão 4.4, constatou-se que, das organizações que confirmaram realizar *backups*, dois terços (254 de 385: 66%) não armazenam os arquivos criptografados, medida de segurança considerada básica para resguardar sua confidencialidade e evitar vazamentos de dados (Figura 15).

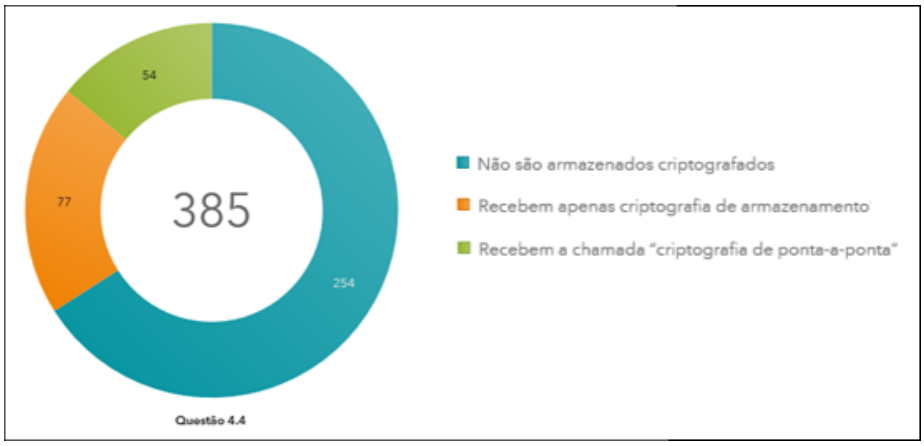


**Figura 15 - Utilização de criptografia no local de armazenamento dos arquivos de *backup*.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

122. Ademais, um quinto das organizações (77 de 385: 20%) usa solução intermediária (criptografia de armazenamento), na qual a cifragem/decifragem ocorre somente no servidor de *backup* (ou no servidor do provedor de "nuvem") e, portanto, os arquivos trafegam em claro na rede da organização (ou na Internet) e, consequentemente, ficam suscetíveis à interceptação. Somente 14% das organizações (54 de 385) adotam a chamada "criptografia de ponta-a-ponta", processo que evita que os dados trafeguem em claro ao realizar a cifragem/decifragem no servidor de origem dos arquivos.

123. Relativamente aos sistemas estruturantes da APF, frisa-se que, por previsão da NC 19/IN01/DSIC/GSIPR[24], estes devem implementar uma série de mecanismos de controle de acesso lógico e respectivas trilhas de auditoria (item 4.3 e subitens).

124. A seu turno, a Questão 4.8 identificou uma situação de risco potencial à medida que pouco mais da metade das organizações (179 de 348: 51,4%) não guardam os registros dos acessos realizados ao ambiente segregado que armazena os *backups*, os quais podem ser necessários para tratar eventuais incidentes de segurança envolvendo aquele local.

Critério

125. *Framework* de controles críticos de SegCiber do CIS, controle 10 (*Data Recovery Capabilities*), subcontrole 10.4 – *Protect Backups* (Tabela 2).

Efeitos

126. A ausência de implementação de controles criptográficos sobre os arquivos dos *backups* potencializa o risco de vazamento de dados e informações, sobretudo sensíveis e/ou sigilosos, tendo em vista que, se a organização sofrer um incidente de exfiltração de dados, esses estarão em claro.

127. Adicionalmente, a ausência de registro dos *logs* de acesso ao local em que os *backups* são armazenados pode inviabilizar o tratamento de incidentes de segurança envolvendo esse ambiente.

Boas práticas

128. Uma prática altamente recomendada é a implementação do processo conhecido como "criptografia de ponta-a-ponta", o qual, por realizar a cifragem/decifragem no servidor de origem dos arquivos, evita que os dados trafeguem em claro na Internet ou mesmo na rede interna da organização.

Benefícios esperados

129. As organizações que protegem adequadamente seus *backups*, por exemplo criptografando os respectivos arquivos, resguardam a confidencialidade dos seus dados e informações e, consequentemente, previnem a ocorrência de incidentes de vazamento de dados, sobretudo sigilosos.

130. A proteção do ambiente de armazenamento das cópias de segurança, a seu turno, mitiga a ocorrência de incidentes de segurança relacionados a esse local.

2.6. Subcontrole 5: Armazene as cópias de segurança (*backups*) da organização em ao menos um destino não acessível remotamente

131. Como visto no subcontrole anterior, à medida que as organizações foram adquirindo mais maturidade e começaram a se proteger de ataques de *ransomware* por meio da realização de cópias periódicas dos seus dados e sistemas, os *malwares* passaram a incluir os próprios arquivos de *backup* entre os seus alvos principais.

132. Com isso, além da proteção física e lógica do local de armazenamento dos *backups* (subcontrole 4), fez-se necessário garantir que ao menos uma cópia desses arquivos fosse armazenada e mantida totalmente *off-line*, isto é, desconectada do espaço cibernético e, portanto, inacessível pela rede da organização, seja por meio de chamadas de sistema operacional, de chamadas de API (*Application Programming Interface*) ou por qualquer outro meio de acesso remoto.

133. Idealmente, realiza-se esse armazenamento em fitas próprias para *backup* (*e.g.* fitas LTO) ou em discos rígidos (*hard drives*, ou HDs). Entretanto, organizações de menor porte podem fazer uso de dispositivos mais acessíveis (DVDs, CDs, *pendrives*), caso em que o risco de vazamento de dados ou de comprometimento dos arquivos aumenta significativamente, pois tais objetos podem, facilmente, ser diretamente extraviados ou, então, inseridos em microcomputadores/*notebooks* conectados à rede, perdendo, assim, sua característica *off-line*.

Questão 5.1

134. Essa questão objetivou verificar se os *backups* são mantidos em ao menos um destino não acessível remotamente.

Questões 5.2 e 5.3

135. Essas questões buscaram identificar o tipo de mídia não acessível remotamente em que são armazenados os *backups* tanto da principal base de dados quanto dos servidores/máquinas que hospedam o principal sistema da organização. As respostas são mostradas na Tabela 5.

**Tabela 5 - Tipo de mídia em que são armazenados os *backups*.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

| **Mídia não acessível remotamente com os *backups*** | **Da principal base de dados** | **Dos servidores/máquinas do principal sistema** |
|---|---|---|
| Fita | 126 | 98 |
| Disco rígido (HD) | 28 | 20 |
| Outra mídia | 2 | 3 |
| **TOTAL** | **156** | **121** |

136. Percebe-se que a maioria das organizações (126 de 156: 80,8%) armazena suas cópias de segurança em fitas de *backup*, que são um tipo de mídia significativamente mais complicado de acessar do que os discos rígidos. Em todo caso, por oportuno, reforça-se novamente, que, com vistas a se evitar vazamentos de dados, a adoção de controles lógicos (criptográficos) tende a ser mais efetiva do que a implementação de mecanismos de proteção física (parágrafo 107).

**Achado 7 - A organização não armazena suas cópias de segurança (*backups*) em ao menos um destino não acessível remotamente**

Situação encontrada

137. A Questão 5.1 registrou que mais da metade das organizações auditadas (247 de 410: 60,2%) não adotam a boa prática de manter seus *backups* em ao menos um destino não acessível remotamente (Figura 16). No entanto, é preciso descontar desse número as 25 organizações que declararam que sequer realizam *backups* (parágrafo 109).

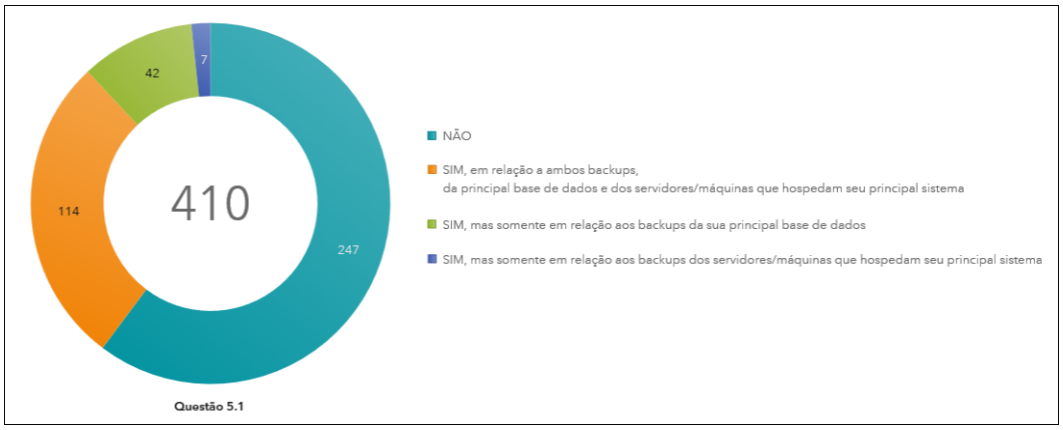


**Figura 16 - A organização mantém seus *backups* em ao menos um destino não acessível remotamente?**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 3])

138. Analisando-se exclusivamente as organizações que cumprem essa prática, tem-se que um quarto (42 de 163: 25,8%) afirmou fazê-lo apenas em relação aos *backups* da sua principal base de dados e 4,3% (7 de 163) disseram implementá-la tão somente em relação às cópias dos servidores/máquinas que hospedam seu principal sistema, ao passo que a grande maioria (114 de 163: 69,9%) declarou que mantém instâncias de ambos os *backups* inacessíveis remotamente.

Critério

139. *Framework* de controles de SegCiber do CIS, controle 10 (*Data Recovery Capabilities*), subcontrole 10.5 – *Ensure All Backups Have at Least One Offline Backup Destination* (Tabela 2).

Efeitos

140. Manter ao menos uma cópia dos *backups* totalmente inacessível por meio de acesso remoto atua para blindar essa instância de ataques exclusivamente cibernéticos. Contrariamente, a não implementação desse controle acarreta o risco de que os próprios arquivos dos *backups* acabem sendo corrompidos, excluídos ou criptografados por um criminoso ou um *malware* e, consequentemente, o processo de *backup* da organização seja tornado sem efeito e esta não consiga se recuperar de um ataque.

Benefícios esperados

141. A organização que mantém cópias dos seus *backups* inacessíveis remotamente adiciona mais uma camada de segurança ao seu processo de *backup*, aumentando, assim, sua resiliência em relação a incidentes cibernéticos e *malwares*, em especial quanto a ataques do tipo *ransomware*.

**Evidências, análises, causas e encaminhamentos dos achados**

142. Tendo em vista que essas seções acabariam sendo muito similares, ponderou-se preferível apresentá-las de modo unificado, ao final, do que as repetir dentro da estrutura de cada achado individual.

143. As evidências que suportam todos os achados foram submetidas pelos respondentes designados pelas organizações para responderem o questionário da auditoria. Nos casos em que as evidências são as próprias respostas fornecidas a perguntas do questionário, o número da questão envolvida é mencionado na seção "Situação encontrada", cujo texto também traz as análises realizadas.

144. Adicionalmente, o questionário solicitou que fossem anexados documentos específicos relativos aos achados identificados, a exemplo das políticas de *backup* (Achado 1) e de evidências dos *backups* automatizados da principal base de dados (Achado 2 - Questão 1.7), dos *backups* integrais do principal sistema (Achado 3 - Questão 2.6), dos planos de *backup* (Achado 4 - Questão 2.8), dos testes de restauração (Achado 5 - Questões 3.3, 3.5 e 3.6), dos mecanismos de proteção física e *logs* de acesso ao ambiente segregado (Achado 6 - Questões 4.7 e 4.9) e das mídias não

acessíveis remotamente (Achado 7 - Questões 5.4 e 5.5). Todas essas evidências foram analisadas pelos auditores e geraram comentários especificamente direcionados a cada organização nos respectivos relatórios de *feedback*.

145. À exceção dos achados positivos (2 e 3), os demais têm por causa, de modo geral, a baixa maturidade das organizações quanto à gestão de SegInfo, que acaba por se refletir na carência de implementação de controles específicos de SegCiber, em especial aqueles relativos aos procedimentos e rotinas de *backup*. Essa falta de maturidade é agravada pela ausência de normativos que orientem e direcionem os gestores das organizações no que tange à implementação desses controles.

146. Essa constatação, inclusive, foi evidenciada a partir do estudo da correlação entre o iSegInfo, indicador usado para medir a maturidade em gestão de SegInfo (obtido no âmbito do Levantamento Integrado de Governança Organizacional Pública realizado pelo TCU em 2018), e um índice criado especificamente para aferir o nível de adoção dos controles de *backup*/*restore* (parágrafo 193).

147. Assim, considerando que, em maior ou menor grau, os achados compartilham a mesma causa, o encaminhamento deles derivado, em essência, volta-se a atenuá-la. Com esse intuito, propõe-se recomendar aos Órgãos Governantes Superiores (OGS) dos Poderes Executivo e Judiciário, bem como do Ministério Público, que editem normativos para endereçar as questões abordadas neste relatório em relação às entidades e órgãos públicos sob os seus respectivos âmbitos de governança.

2.7. Avaliação pessoal do respondente sobre a aderência da organização aos subcontroles

148. Após a primeira parte com perguntas gerais sobre a organização (Seção 2.1) e as cinco abas contendo perguntas específicas sobre os subcontroles do controle 10 do *framework* do CIS (Seções 2.2 a 2.6), o questionário instava os gestores a avaliarem suas próprias organizações, atribuindo-lhes notas, numa escala de 1 a 10, para os respectivos níveis de aderência em relação a cada um desses cinco subcontroles (Seção 2.7; Anexo I - Questionário da Auditoria sobre *backup*, Questão 6.1).

149. A intenção inicial da equipe de auditores era usar essas autoavaliações dos gestores para, em conjunto com as demais respostas preenchidas no questionário, comparar os níveis de maturidade entre as organizações auditadas. Contudo, após análise de diversas dessas respostas, concluiu-se que seu grau de subjetividade não permitiria que servissem a esse propósito comparativo.

150. Em muitos casos, percebeu-se que os gestores haviam superavaliado as notas atribuídas na Questão 6.1, posto que estas não se mostravam compatíveis com as próprias respostas fornecidas nas perguntas anteriores do questionário. Assim sendo, optou-se por desconsiderar essa avaliação para fins de comparação entre as organizações, utilizando-se, para esse propósito, um indicador de qualidade (iBackup) derivado das respostas ao questionário relativas aos cinco subcontroles (Capítulo 4).

151. Nada impede, contudo, que cada gestor utilize suas autoavaliações para nortear o incremento de maturidade da sua própria organização ao longo dos próximos anos. Inclusive, para ajudar nesse processo, esta auditoria incluiu a elaboração e o encaminhamento, às organizações auditadas, de dois tipos distintos de relatórios de *feedback*, um contendo análises e sugestões em relação às respostas fornecidas individualmente pela organização e outro a situando comparativamente em um universo de organizações similares. Esses relatórios também são detalhados no Capítulo 4 (parágrafos 182-185).

152. Adicionalmente, o questionário permitiu que os gestores registrassem suas percepções sobre os principais desafios, deficiências e pontos de atenção relacionados à execução dos procedimentos de *backup* e *restore* nas suas respectivas organizações, bem como quaisquer outras considerações que entendessem pertinentes (Anexo I - Questionário da Auditoria sobre *backup*, Questão 6.2). Os comentários mais relevantes estão no Capítulo 6 (parágrafos 215-224).

**3. Painel para visualização gráfica das respostas fornecidas pelas organizações**

153. Esta auditoria incluiu a criação de um painel de consulta interativa – utilizando a ferramenta SAS Visual Analytics – para permitir a visualização gráfica das informações fornecidas pelas organizações auditadas em resposta ao questionário sobre seus procedimentos de *backup* e *restore*.

Ressalva-se que, por conter informações sensíveis, o acesso ao painel ficou restrito à equipe de auditores.

154. Além de mostrar a situação observada na auditoria, esse painel será utilizado, futuramente, para possibilitar que o TCU continue acompanhando de modo efetivo a implementação dos controles de *backup* por parte das organizações da APF, tendo em vista que a presente fiscalização já contribuiu para induzir melhorias nas organizações participantes (Tabela 7, Questões 3 a 5) e que novas avaliações sobre este mesmo tema ainda devem ser realizadas pelo Tribunal, ainda que sob a forma de disponibilização de um serviço de autoavaliação (Tabela 7, Questão 6).

155. O painel foi estruturado em oito abas de visualização: "Introdução", "Organizações, questões e filtros", "Porte e política de *backup*", "Subcontrole 1", "Subcontrole 2", "Subcontrole 3", "Subcontrole 4" e "Subcontrole 5".

Aba "Introdução"

156. A aba "Introdução" apresenta uma descrição sucinta da auditoria e do método utilizado (CSA), além de enumerar os cinco subcontroles avaliados (Figura 17).

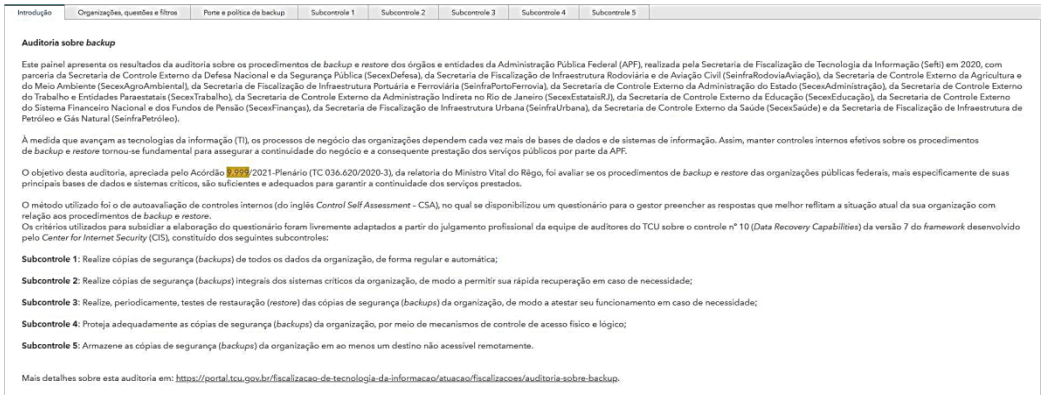


**Figura 17 - Painel "Auditoria sobre *backup*" - Aba "Introdução".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Organizações, questões e filtros"

157. Essa aba lista todas as 410 organizações que responderam o questionário da auditoria, transcreve os textos das questões aplicadas no âmbito de cada um dos cinco subcontroles avaliados e explica os filtros que foram criados para permitir uma visualização interativa dos resultados (Figura 18).

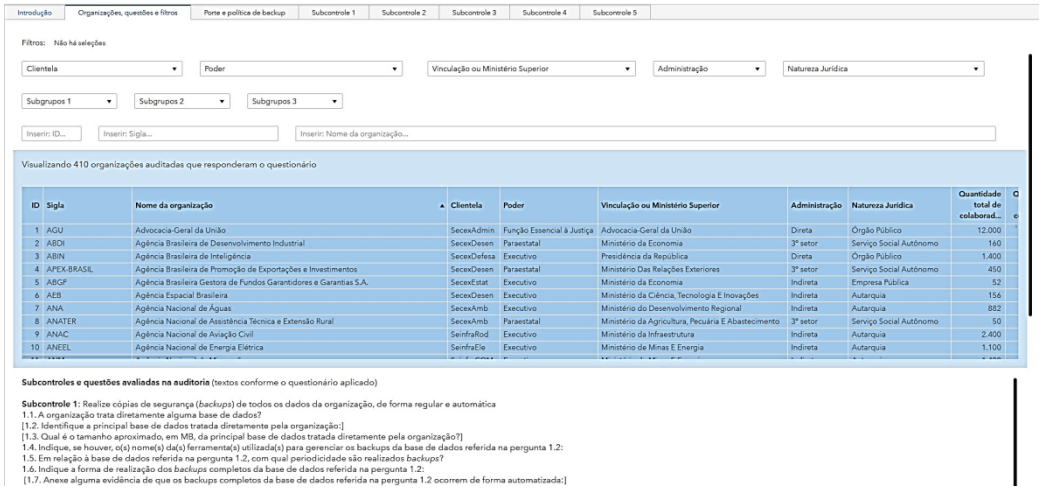


**Figura 18 - Painel "Auditoria sobre *backup*" - Aba "Organizações, questões e filtros".**
(Fonte: painel construído para visualizar as respostas das organizações)

158. A tabela desta aba, bem como os gráficos das demais abas, são todos dinâmicos, o que significa que o universo dos dados apresentados pode ser alterado com base na aplicação dos filtros disponíveis, restringindo-se interativamente a visualização das respostas das organizações de modo a mostrar apenas aquelas que atendem o(s) critério(s) selecionado(s). É possível, inclusive, combinar essas filtragens, ou seja, aplicar múltiplos filtros simultaneamente.

159. Os filtros disponíveis são:

159.1. Clientela: filtra as organizações da clientela de uma mesma unidade técnica do TCU;

159.2. Poder: "Executivo", "Judiciário", "Legislativo", "Paraestatal", "Função Essencial à Justiça" ou "GDF";

159.3. Vinculação ou Ministério Superior: filtra as organizações distintas que são vinculadas a um mesmo ente hierarquicamente superior;

159.4. Administração: "Direta", "Indireta" ou "3º Setor";

159.5. Natureza Jurídica: "Autarquia", "Empresa Pública", "Fundação", "Órgão Público", "Serviço Social Autônomo" ou "Sociedade de Economia Mista";

159.6. Subgrupos: três filtros adicionais que foram configurados com subgrupos de organizações similares (Anexo III - Subgrupos de organizações com certa similaridade), de modo que se possa visualizar como estão quando comparadas entre si.

160. A partir da aplicação dos filtros descritos, as respostas das organizações auditadas podem ser visualizadas e comparadas com base em diversos critérios distintos, permitindo, assim, ampla segmentação das análises. Esses filtros, inclusive, foram usados para gerar os gráficos que ilustram alguns dos relatórios de *feedback* a serem enviados às organizações participantes (parágrafo 185).

Aba "Porte e política de *backup*"

161. A aba "Porte e política de *backup*" apresenta os gráficos relativos às respostas às três primeiras perguntas do questionário, que versavam sobre o porte da organização – em termos da quantidade total de colaboradores e da quantidade de colaboradores do setor de TI – e sobre a existência ou não de política de *backup*, mesmo que ainda não aprovada formalmente (Seção 2.1).

162. Para o conjunto das 410 organizações que responderam o questionário, o primeiro gráfico ("Porte da organização - Quantidade total de colaboradores") pode ser visualizado na Figura 2, na qual se percebe que as seis maiores organizações auditadas, de acordo com esse critério, foram: Exército Brasileiro (EB), Empresa Brasileira de Correios e Telégrafos (ECT), Banco do Brasil (BB), Caixa Econômica Federal (Caixa), Comando da Marinha (CM) e Comando da Aeronáutica (Comaer).

163. Entretanto, quando se considera apenas as equipes de TI (gráfico "Porte da organização - Quantidade de colaboradores do setor de TI"), além dos bancos federais (BB e Caixa), também figuram na relação das quatro maiores organizações as empresas estatais que prestam serviços de custódia e tratamento de dados para a APF: Serviço Federal de Processamento de Dados (Serpro) e Empresa de Tecnologia e Informações da Previdência – Dataprev (Figura 3).

164. O terceiro gráfico ("Política de *backup*"), a seu turno, mostra a distribuição das organizações auditadas conforme a existência ou não de política de *backup* (Figura 4).

Aba "Subcontrole 1"

165. A aba "Subcontrole 1" apresenta os gráficos de distribuição das respostas às seguintes perguntas relativas ao "Subcontrole 1: Realize cópias de segurança (*backups*) de todos os dados da organização, de forma regular e automática" (Figura 19):

Questão 1.1) A organização trata diretamente alguma base de dados?

Questão 1.4) Indique, se houver, o(s) nome(s) da(s) ferramenta(s) utilizada(s) para gerenciar os *backups* da base de dados referida na pergunta 1.2 (principal base de dados da organização):

Questão 1.5) Em relação à base de dados referida na pergunta 1.2, com qual periodicidade são realizados *backups* completos/*full* (1.5.1), diferenciais (1.5.2) e incrementais (1.5.3)?

Questão 1.6) Indique a forma de realização (manual/automatizada/outra) dos *backups* completos da base de dados referida na pergunta 1.2:

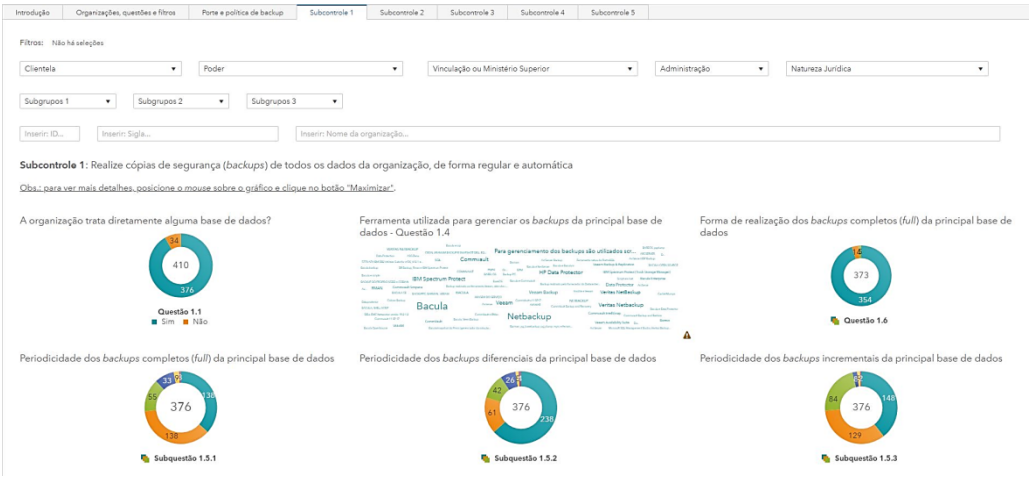


**Figura 19 - Painel "Auditoria sobre *backup* - Aba "Subcontrole 1".**
(Fonte: painel construído para visualizar as respostas das organizações)

166. Os resultados dessas e das demais perguntas do Subcontrole 1 estão na Seção 2.2.

Aba "Subcontrole 2"

167. A aba "Subcontrole 2" mostra os gráficos de distribuição das respostas às seguintes perguntas relativas ao "Subcontrole 2: Realize cópias de segurança (*backups*) integrais dos sistemas críticos da organização, de modo a permitir sua rápida recuperação em caso de necessidade" (Figura 20):

Questão 2.1) A organização hospeda, em servidor ou conjunto de servidores/máquinas próprios, algum sistema cuja gestão está sob sua responsabilidade?

Questão 2.3) Indique, se houver, o(s) nome(s) da(s) ferramenta(s) utilizada(s) para gerenciar os *backups* do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema da organização):

Questão 2.4) Em relação ao servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2, com qual periodicidade são realizados os *backups*?

Questão 2.5) Indique a forma de realização (parcial/integral/outra) dos *backups* do servidor ou conjunto de servidores/máquinas:

Questão 2.7) A organização possui plano de *backup* específico para o sistema referido na pergunta 2.2?

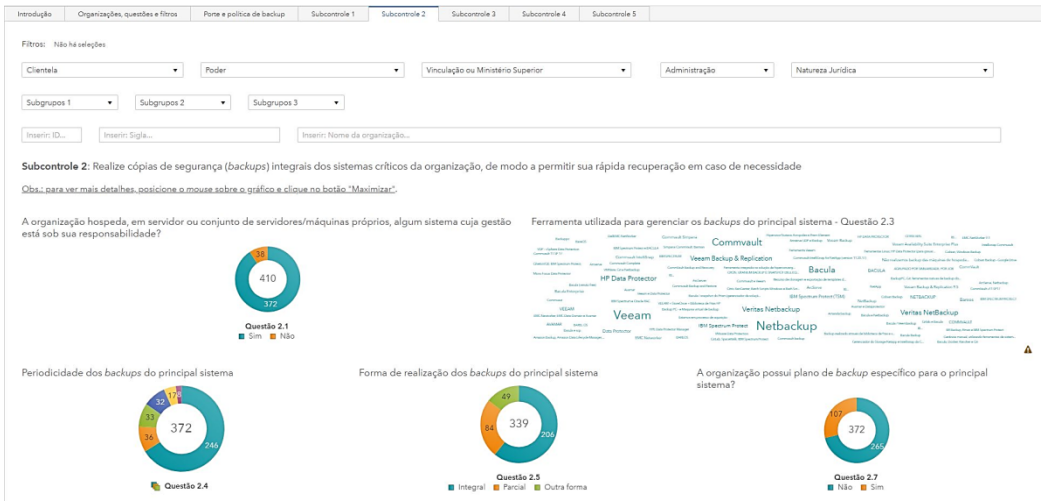


**Figura 20 - Painel "Auditoria sobre *backup* - Aba "Subcontrole 2".**
(Fonte: painel construído para visualizar as respostas das organizações)

168. Os resultados dessas e das demais perguntas do Subcontrole 2 estão na Seção 2.3.

Aba "Subcontrole 3"

169. A aba "Subcontrole 3" traz os gráficos de distribuição das respostas às seguintes perguntas do "Subcontrole 3: Realize, periodicamente, testes de restauração (*restore*) das cópias de segurança (*backups*) da organização, de modo a atestar seu funcionamento em caso de necessidade" (Figura 21):

Questão 3.1) A organização executa, periodicamente, testes de restauração (*restore*) dos seus *backups*?

Questão 3.2) Os testes de restauração (*restore*) são documentados (isto é, geram algum tipo de registro formal ou relatório de resultados)?

Questão 3.4) Com qual periodicidade são realizados os testes de restauração (*restore*) dos *backups* da principal base de dados (3.4.1) e do principal sistema (3.4.2) da organização?

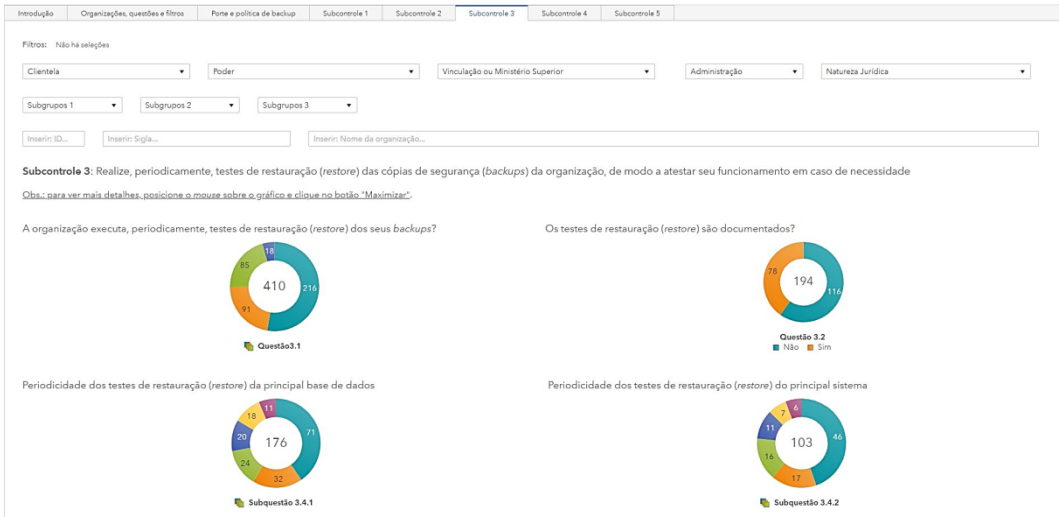


**Figura 21 - Painel "Auditoria sobre *backup* - Aba "Subcontrole 3".**
(Fonte: painel construído para visualizar as respostas das organizações)

170. Os resultados dessas e das demais perguntas do Subcontrole 3 estão na Seção 2.4.

Aba "Subcontrole 4"

171. A aba "Subcontrole 4" apresenta os gráficos de distribuição das respostas às seguintes perguntas relativas ao "Subcontrole 4: Proteja adequadamente as cópias de segurança (*backups*) da organização, por meio de mecanismos de controle de acesso físico e lógico" (Figura 22):

Questão 4.1) Onde são armazenados os arquivos dos *backups* da organização?

Questão 4.4) No local de armazenamento, os arquivos dos *backups* são criptografados?

Questão 4.5) O local de armazenamento dos arquivos dos *backups*, sob gestão da própria organização, considerado o mais seguro pelo respondente, possui mecanismo de controle de acesso físico?

Questão 4.6) A permissão de acesso ao ambiente segregado em questão é concedida a partir de qual critério (algo que somente o usuário sabe, possui, é ou uma combinação desses fatores)?

Questão 4.8) Os acessos ao ambiente segregado são registrados (isto é, há *log* desses acessos, contendo identificador, data/hora e nome da pessoa que acessou)?

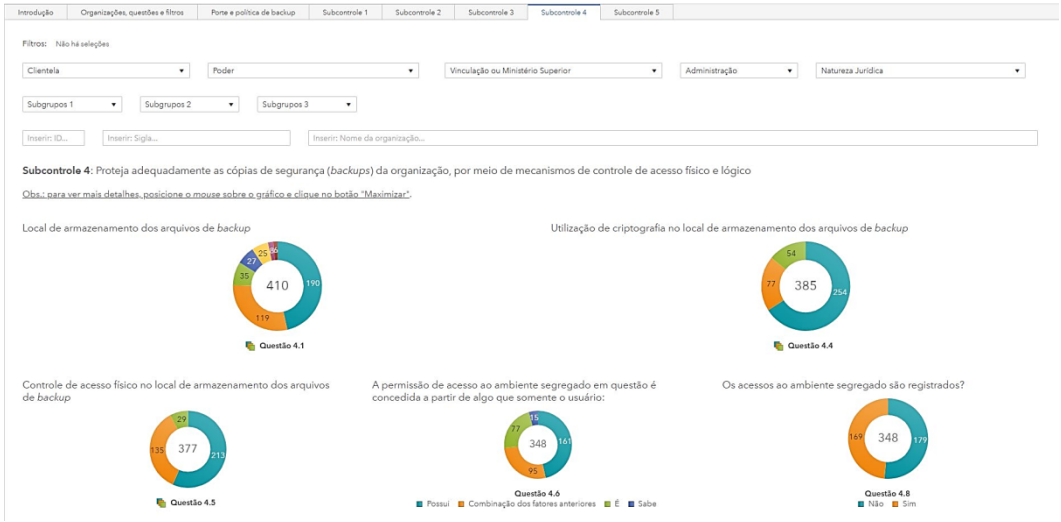


**Figura 22 - Painel "Auditoria sobre *backup* - Aba "Subcontrole 4".**
(Fonte: painel construído para visualizar as respostas das organizações)

172. Os resultados dessas e das demais perguntas do Subcontrole 4 estão na Seção 2.5.

Aba "Subcontrole 5"

173. Por fim, a aba "Subcontrole 5" mostra os gráficos de distribuição das respostas às seguintes perguntas relativas ao "Subcontrole 5: Armazene as cópias de segurança (*backups*) da organização em ao menos um destino não acessível remotamente" (Figura 23):

Questão 5.1) A organização mantém seus *backups* em ao menos um destino não acessível remotamente?

Questão 5.2) Em qual mídia não acessível remotamente são armazenados os *backups* da base de dados referida na pergunta 1.2 (principal base de dados tratada diretamente pela organização)?

Questão 5.3) Em qual mídia não acessível remotamente são armazenados os *backups* do servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2 (principal sistema hospedado pela organização)?

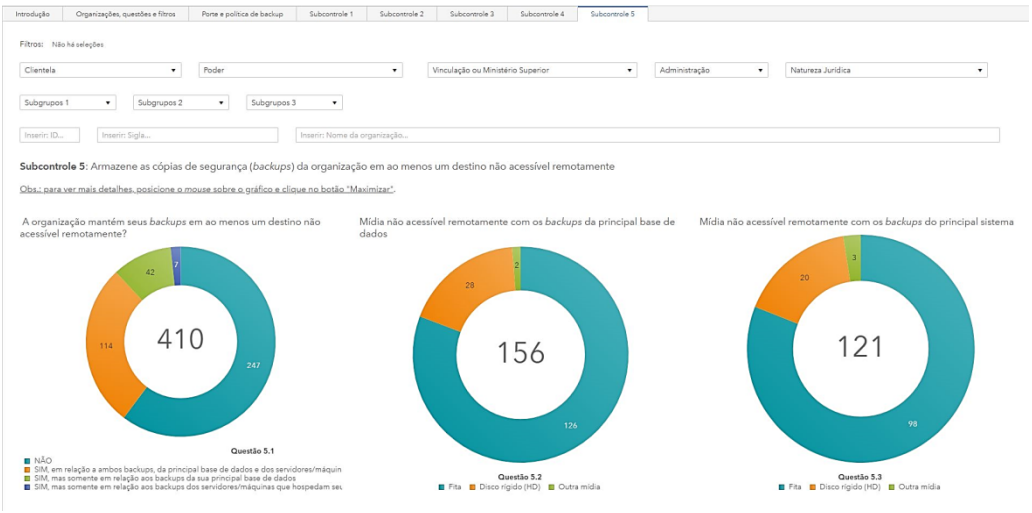


**Figura 23 - Painel "Auditoria sobre *backup* - Aba "Subcontrole 5".**
(Fonte: painel construído para visualizar as respostas das organizações)

174. Os resultados dessas e das demais perguntas do Subcontrole 5 estão na Seção 2.6.

**4. Propósitos da auditoria, relatórios de *feedback* e indicador de qualidade (iBackup)**

175. Por meio do TC 001.873/2020-2, que culminou no Acórdão 4.035/2020-TCU-Plenário (Rel. Min. Vital do Rêgo), a Sefti elaborou amplo levantamento com o objetivo de conhecer a macroestrutura de governança e gestão de SegInfo/SegCiber na APF, incluindo aspectos relativos à legislação, políticas, normativos, atores, papéis e responsabilidades atinentes a essas áreas. O respectivo relatório apontou a necessidade de auditorias específicas para verificar o nível de preparação das organizações públicas em relação a controles críticos de SegCiber, além de conscientizá-las para os problemas e os riscos inerentes.

176. Com isso, e tendo em vista a recente expansão no número de casos de ataques de *ransomware* vivenciada no mundo todo e, em especial, no Brasil[3,18,19], decidiu-se que o primeiro controle a ser verificado seria o relativo à realização de procedimentos de *backup* e *restore*, tendo sido a presente auditoria, inclusive, prevista no âmbito da Estratégia de Fiscalização do TCU em SegInfo e SegCiber, sugerida naquele relatório e aguardando aprovação (Figura 24, Eixo "Diagnosticar").

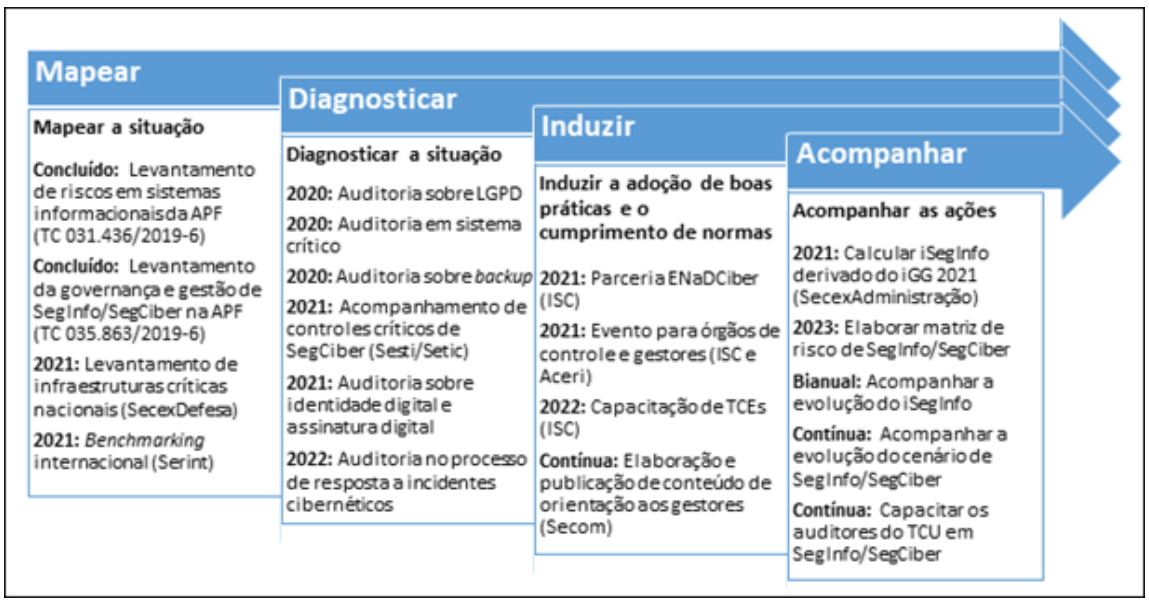


**Figura 24 - Estratégia de Fiscalização do TCU em SegInfo e SegCiber.**
(Fonte: TC 001.873/2020-2, peça 46, Figura 37)

Propósitos da auditoria

177. O propósito geral desta auditoria foi realizar um diagnóstico das organizações da APF quanto à implementação de controles de *backup*/*restore*. Em síntese, esse panorama encontra-se no Capítulo 2, cujas informações serão levadas em consideração na definição de auditorias baseadas em risco (*e.g.* auditar órgãos de maturidade baixa responsáveis por manter sistemas governamentais críticos).

178. Porém, além de gerar esse mapeamento para o Tribunal, a fiscalização também intencionou conscientizar e orientar os gestores das organizações da APF em relação aos riscos associados à ausência dos cinco subcontroles de *backup*/*restore* verificados, a exemplo dos citados ataques de *ransomware* (parágrafo 176; Capítulo 6), bem como, a partir do cenário percebido e das avaliações qualitativas realizadas pelo auditores sobre as evidências recebidas, fundamentar proposta de recomendação para endereçar o aprimoramento desses controles.

179. Como consequência, espera-se perceber, ao longo dos próximos anos, algum incremento na maturidade das organizações da APF, sobretudo daquelas que efetivamente responderam ao questionário da auditoria, relativamente à gestão dos seus procedimentos e rotinas de *backup* e *restore*, com reflexos nas respectivas resiliências quanto a falhas de segurança, vulnerabilidades e ataques cibernéticos.

180. Adicionalmente, a auditoria se prestou a municiar os gestores da área de SegInfo, bem como as unidades de auditoria interna dos órgãos da APF, com uma sistemática (CSA – parágrafos 11-12) e com ferramentas específicas (*e.g.* questionário da auditoria [Anexo I], *checklists* para verificação de política e plano de *backup*, relatórios de *feedback*) para que as organizações continuem se autoavaliando e evoluindo em relação à implementação desses controles.

181. Por fim, relativamente a todos os auditores participantes, a auditoria serviu de aprendizado e de aplicação prática tanto da metodologia de autoavaliação de controles (CSA) quanto do LimeSurvey, ferramenta de questionários eletrônicos utilizada como padrão no TCU, sendo que esses profissionais poderão replicar a experiência em trabalhos futuros nas suas próprias unidades técnicas. Esta fiscalização atuou, também, para conscientizá-los da importância dos procedimentos de *backup*/*restore* para a continuidade do negócio das organizações que compõem a clientela das suas secretarias, podendo impactar, por exemplo, sistemas críticos que suportam as políticas públicas por eles auditadas.

Relatórios de *feedback* às organizações

182. Esta auditoria envolveu a elaboração de dois tipos diferentes de relatórios de *feedback*, os quais serão encaminhados às organizações que responderam o questionário.

183. O primeiro ("Relatório Individual de Autoavaliação") registra as respostas fornecidas pela própria organização e, com o intuito de ajudar os gestores a evoluírem, ao longo dos próximos anos, cada um dos subcontroles avaliados, traz comentários e sugestões dos auditores derivadas das análises das respostas individuais e de todo o conjunto das evidências encaminhadas (parágrafo 144). Especificamente em relação às análises das políticas e planos de *backup*, houve padronização por meio da elaboração de *checklists* (Anexo IV - *Checklists* para verificação de política e plano de *backup*).

184. Adicionalmente, esse relatório comunica às organizações a Estratégia de Fiscalização do TCU em SegInfo e SegCiber (Figura 24), antecipa uma perspectiva de futuras auditorias (*e.g.* outros controles críticos de SegCiber do *framework* do CIS, implementação da LGPD e processo de resposta a incidentes cibernéticos) e avalia as políticas e os planos de *backup* eventualmente submetidos.

185. O segundo ("Relatório Comparativo de *Feedback*") realiza uma avaliação comparativa, com base nos subgrupos de organizações que foram previamente definidos (Anexo III - Subgrupos de organizações com certa similaridade), de modo que os gestores tenham condições de comparar suas próprias realidades (retratadas nos relatórios individuais) com aquelas de um conjunto de organizações similares e, assim, também se sintam motivados a trabalhar para aperfeiçoar os referidos subcontroles. Os gráficos que compõem esses relatórios foram extraídos do painel descrito no Capítulo 3.

Indicador de qualidade dos procedimentos de *backup*/*restore* (iBackup)

186. De modo a permitir a realização de comparações entre as organizações auditadas no que tange à qualidade geral dos respectivos procedimentos de *backup*/*restore*, fez-se necessário resumir em um único valor numérico os dados coletados do conjunto de respostas fornecidas por cada organização.

187. Assim, para compor esse indicador (iBackup), foram selecionadas as respostas a seis perguntas, no total: a que questionou sobre a existência ou não de política de *backup* no âmbito da organização e uma pergunta relacionada a cada um dos cinco subcontroles avaliados na auditoria. Às possíveis respostas a tais perguntas foram atribuídas as notas "0", "1" ou "2", sendo que o valor final do indicador corresponderia, então, à soma das notas individuais obtidas em cada uma das seis respostas. Ou seja, para cada organização, tem-se que o respectivo iBackup pode variar de 0, no mínimo (nota "0" em todas as seis perguntas), a 12, no máximo (nota "2" em todas as seis perguntas).

188. Vale salientar que o objetivo da criação desse indicador foi obter um parâmetro que permitisse realizar comparações objetivas entre as organizações, procurando-se, assim, definir uma sistemática de cálculo bem simples para o iBackup. A Tabela 6 apresenta as seis perguntas selecionadas do questionário, suas correspondentes opções de resposta e as notas atribuídas a cada uma delas.

**Tabela 6 - Composição do indicador de qualidade dos procedimentos de *backup*/*restore* (iBackup).**
(Fonte: elaboração própria, com base nas respostas ao questionário da auditoria)

| **Pergunta escolhida para compor o iBackup** | **Opção de resposta** | **Nota** |
|---|---|---|
| A organização possui política de *backup* (ou instrumento normativo equivalente) documentada e aprovada formalmente? | NÃO | 0 |
| | SIM, existe política de *backup* documentada, porém ainda não aprovada formalmente | 1 |
| | SIM, existe política de *backup* documentada e já aprovada formalmente | 2 |
| 1.5. Em relação à base de dados referida na pergunta 1.2, com qual periodicidade são realizados backups: Completos (*full*)? | Não são realizados | 0 |
| | Ocasionalmente (menos do que uma vez por mês) | |
| | Mensalmente | 1 |
| | Semanalmente | |
| | Diariamente | 2 |
| | Mais de uma vez por dia | |
| 2.4. Em relação ao servidor ou conjunto de servidores/máquinas que hospedam o sistema referido na pergunta 2.2, com qual periodicidade são realizados os backups? | Não são realizados | 0 |
| | Ocasionalmente (menos do que uma vez por mês) | |
| | Mensalmente | 1 |
| | Semanalmente | |
| | Diariamente | 2 |
| | Mais de uma vez por dia | |
| 3.1. A organização executa, periodicamente, testes de restauração (*restore*) dos seus *backups*? | NÃO | 0 |
| | SIM, mas somente em relação aos *backups* de sua principal base de dados | 1 |
| | SIM, mas somente em relação aos *backups* das máquinas que hospedam seu principal sistema | |
| | SIM, em relação a ambos os *backups*, da principal base de dados e dos servidores/máquinas que hospedam seu principal sistema | 2 |

| | | |
|---|---|---|
| 4.4. No local de armazenamento, os arquivos dos *backups*: | Não são armazenados criptografados | 0 |
| | Recebem apenas criptografia de armazenamento | 1 |
| | Recebem a chamada "criptografia de ponta-a-ponta" | 2 |
| 5.1. A organização mantém seus *backups* em ao menos um destino não acessível remotamente? | NÃO | 0 |
| | SIM, mas somente em relação aos *backups* da sua principal base de dados | 1 |
| | SIM, mas somente em relação aos *backups* das máquinas que hospedam seu principal sistema | |
| | SIM, em relação a ambos os *backups*, da principal base de dados e dos servidores/máquinas que hospedam seu principal sistema | 2 |

189. Um dos motivos que levou à criação do iBackup foi buscar demonstrar, de forma simples e imediata, a existência de uma correlação entre a maturidade de uma organização em gestão de SegInfo, de modo geral, e a implementação, na prática, de controles específicos de SegCiber (no caso desta auditoria, dos cinco subcontroles relacionados às rotinas de *backup*/*restore* avaliadas). Em outras palavras, a ideia foi mostrar que organizações mais maduras em gestão de SegInfo tendem a adotar boas práticas quando se trata de controles específicos.

190. Com esse propósito, dentre as 410 organizações que responderam o questionário, foram selecionadas apenas as 344 que responderam "Sim" às perguntas 1.1 (tratam diretamente alguma base de dados) e 2.1 (hospedam em infraestrutura de TI própria algum sistema cuja gestão está sob sua responsabilidade) e que, adicionalmente, haviam participado do Levantamento Integrado de Governança Organizacional Pública realizado pelo TCU em 2018 (TC 015.268/2018-7).

191. Destaca-se que, no âmbito daquele levantamento, foi calculado, dentre outros indicadores, o iSegInfo, cujos resultados foram, também, analisados no âmbito do Levantamento da Governança e Gestão de SegInfo/SegCiber da APF, realizado pela Sefti em 2020 (TC 001.873/2020-2). Os valores do iSegInfo permitiam classificar as organizações em quatro estágios de maturidade: "Inexpressivo", "Iniciando", "Intermediário" e "Aprimorado".

192. A Figura 25, então, apresenta a distribuição das 344 organizações mencionadas nesses quatro estágios e mostra que o estágio "Intermediário" concentra mais de um terço destas.

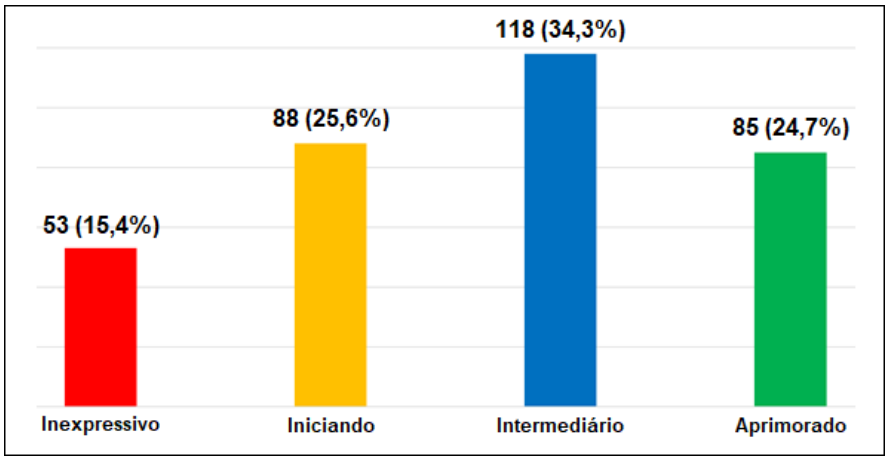


**Figura 25 - Distribuição das organizações auditadas por estágios de capacidade em gestão de SegInfo.**
(Fonte: elaboração própria, com base nas respostas ao questionário da auditoria e no iSegInfo 2018)

193. Conforme ilustrado nas Figuras 26 e 27, verifica-se que as médias de iBackup aumentam conforme os estágios de gestão de SegInfo evoluem, o que permite concluir que, efetivamente, as

organizações com maior maturidade em gestão de SegInfo tendem a adotar as boas práticas de *backup*/*restore* avaliadas nesta auditoria.

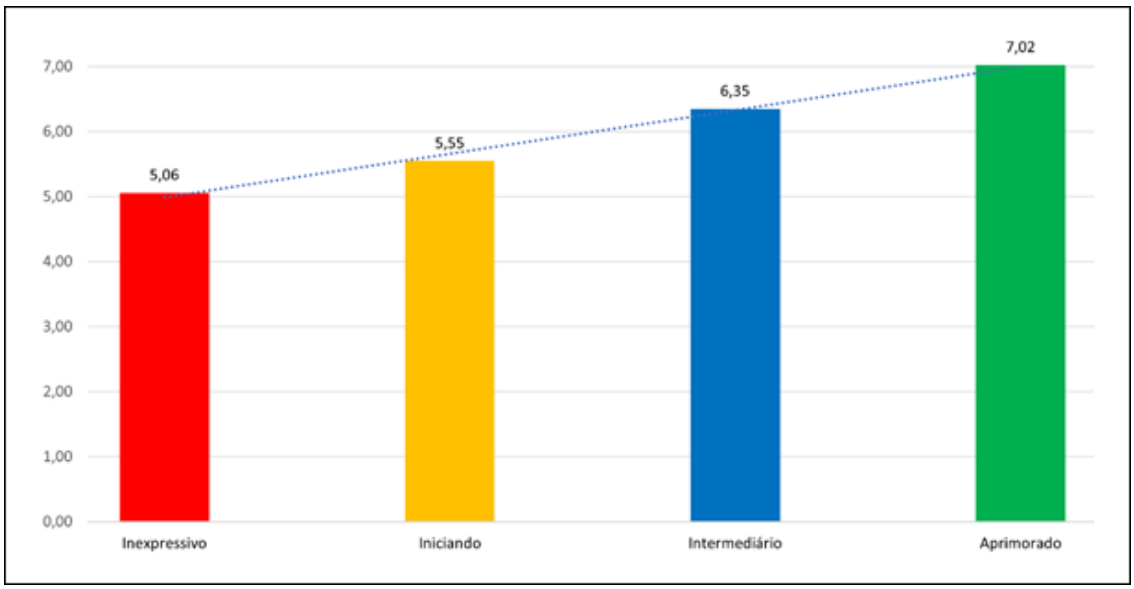


**Figura 26 - Médias de iBackup por estágios de capacidade em gestão de SegInfo.**
(Fonte: elaboração própria, com base nas respostas ao questionário da auditoria e no iSegInfo 2018)

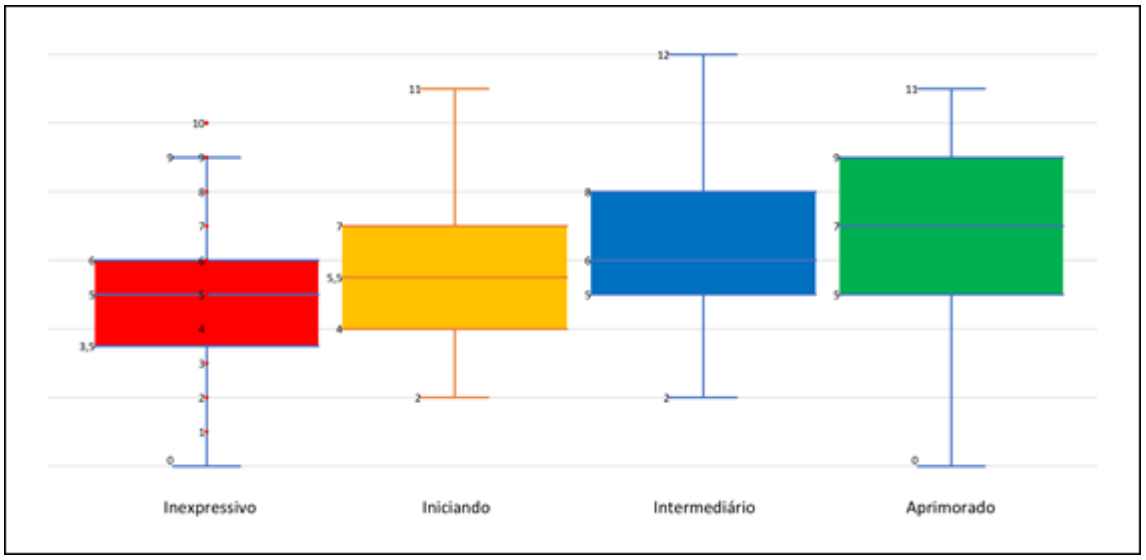


**Figura 27 - Distribuição dos valores de iBackup em cada estágio de capacidade em gestão de SegInfo.**
(Fonte: elaboração própria, com base nas respostas ao questionário da auditoria e no iSegInfo 2018)

## 5. Boas práticas identificadas

194. De acordo com o Manual de Auditoria Operacional do TCU, o relatório de auditoria não deve focar somente nas deficiências e nas falhas encontradas, mas deve, também, registrar boas práticas e esforços desenvolvidos pelos auditados. As boas práticas, inclusive, podem subsidiar a proposição de recomendações, de modo a serem disseminadas para outras organizações em situações similares.

195. Assim, são registradas, a seguir, algumas boas práticas identificadas no decorrer da auditoria.

Plano de Continuidade de Negócio (PCN)

196. A norma ABNT NBR ISO/IEC 27002:2013 (Tecnologia da Informação – Técnicas de segurança – Código de prática para controles de segurança da informação)[xxi], em seu item 17 (Aspectos da segurança da informação na gestão da continuidade do negócio), traz diversos controles e diretrizes relacionados ao planejamento, à implementação e à constante avaliação da continuidade da segurança da informação de uma organização, incluindo a implementação de redundâncias com vistas a atender requisitos de disponibilidade.

197. Mais especificamente, a norma ABNT NBR 15999-1:2007 (Gestão de continuidade de negócios – Parte 1: Código de prática) detalha a gestão da continuidade de negócios (GCN), processo que agrega valor a qualquer organização, visto que, a despeito do porte, todas estão sujeitas à ocorrência de interrupções, por diversas razões (falhas tecnológicas, desastres naturais, problemas no fornecimento de serviços públicos, incidentes de segurança, ataques cibernéticos, atos de terrorismo etc.).

198. Assim sendo, identificou-se, como boa prática citada por uma das organizações auditadas, a manutenção de Planos de Continuidade de Negócio (PCN), que incluem, em alguns casos, a previsão de medidas de contingência voltadas especificamente a assegurar a continuidade da operação de determinados sistemas/plataformas tecnológicas, a exemplo da realização de procedimentos de recuperação (*restore*) de cópias de segurança (*backups*), quando necessário.

199. Entre outros itens, tais planos devem especificar quem são os responsáveis em casos de crise e seus contatos, prever os eventos de diferentes graus de gravidade/dano e delinear ações de contingência e roteiros de resposta para cada um desses cenários ("ação", "quem", "onde", "como" e "resultado esperado"). Com isso, caso se materialize algum dos sinistros previstos, a organização já tem definidos e treinados os respectivos responsáveis, bem como os procedimentos a serem ser realizados, diminuindo, consequentemente, o tempo de reação e mitigando os prejuízos advindos desses episódios.

Espelhamento dos bancos de dados/sistemas

200. Além das ferramentas usuais de *backup*, o uso de bancos de dados e servidores espelhados em tempo real é uma boa prática, utilizada por algumas das organizações auditadas, que diminui os tempos de reação e de retorno à atividade "normal" na eventual ocorrência de sinistro, tendo em vista que, por exemplo, nos casos de falha, o banco de dados/máquina/servidor espelhado pode ser programado para assumir a operação quase que instantaneamente no lugar do ativo principal.

201. Para as organizações que possuem volumes menores de dados, em especial, essa prática mostra-se bastante útil.

Testes de recuperação (*restore*) aleatórios

202. Pode ser proibitivamente caro, ou mesmo inviável, realizar testes de recuperação (*restore*) periódicos sobre todas as bases de dados, arquivos e sistemas da organização, sobretudo à medida que se passa a realizar esses testes mais frequentemente.

203. Assim, algumas organizações "sorteiam" as bases de dados/sistemas a serem testados em cada período, em regime de rodízio, assegurando, com isso, que, com alguma periodicidade, pelo menos, todas(os) acabem sendo testados.

## 6. Informações complementares

204. Este capítulo relata alguns incidentes de SegInfo relacionados ao objeto da auditoria que, coincidentemente, ocorreram no seu transcurso, bem como sintetiza a atuação do CTIR Gov na coordenação das respectivas respostas. Traz, ainda, comentários relevantes registrados pelos gestores que responderam o questionário, bem como os resultados de uma avaliação da condução em si da auditoria, submetida a esses mesmos gestores após a fase de execução.

Incidentes de segurança da informação ocorridos no curso da auditoria

205. Durante a execução da auditoria, conforme amplamente noticiado na mídia[xxii], ocorreram diversos ataques cibernéticos que causaram indisponibilidade de serviços de TI em órgãos públicos, a exemplo do Superior Tribunal de Justiça (STJ), do Conselho Nacional de Justiça (CNJ),

da Controladoria-Geral da União (CGU), do Ministério da Saúde (MS), do Governo do Distrito Federal (GDF), do Conselho Federal de Contabilidade (CFC) e da Prefeitura Municipal de Vitória - ES.

206. O STJ considerou ter sofrido "o pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade". A resposta a esse episódio, que mobilizou "mais de 50 servidores do [seu] quadro permanente", contou com o suporte e o apoio técnico de "oito fabricantes de tecnologia (*hardware* e *software*)" e envolveu a colaboração da Polícia Federal (PF), do Comando de Defesa Cibernética (ComDCiber) do EB e do Serpro na investigação[xxiii], ilustra bem a necessidade de as organizações realizarem e manterem *backups* completos e atualizados, de acordo com as práticas avaliadas nesta auditoria.

207. No dia 4/11/2020, o STJ divulgou ter detectado, na tarde do dia anterior, uma invasão na sua rede de informática e que, consequentemente, seriam suspensas, até 9/11/2020, as audiências, "todas as sessões de julgamento por videoconferência e também as sessões virtuais destinadas à apreciação de recursos internos"[xxiv], tendo remetido notícia-crime ao Ministério da Justiça e Segurança Pública (MJSP), a qual foi encaminhada à PF para instauração de inquérito[xxv]. No dia seguinte (5/11/2020), novo comunicado confirmou o ataque e reafirmou o regime de plantão instaurado na Corte[xxvi].

208. A partir do dia 9/11/2020, de forma gradual, os principais serviços e sistemas foram voltando a funcionar, sendo noticiada a recuperação total somente em 19/11/2020[xxvii]. O ataque, além de causar indisponibilidade de serviços, foi utilizado para acessar arquivos e copiar dados do Tribunal[xxviii].

209. Embora não confirmado oficialmente pelo STJ, provavelmente se tratou de um ataque de *ransomware*, com sequestro de dados e cobrança de resgate[xxix], sendo que os comunicados divulgados revelam que o *backup* íntegro foi crucial para o Tribunal recuperar os dados e restabelecer os serviços[xxx].

210. A ABNT NBR ISO/IEC 27002:2013[25], em seu item 12.3.1 (Cópias de segurança das informações), recomenda que "os recursos adequados para a geração de cópias de segurança sejam disponibilizados para garantir que toda informação e os *softwares* essenciais possam ser recuperados após um desastre ou a falha de uma mídia". No caso específico do STJ, o desastre foi digital, na forma de um ataque cibernético, e a recuperação do ambiente só foi possível graças aos *backups*.

211. Assim, em um mundo progressivamente mais digitalizado, realizar e testar rotinas de *backup* deixam de ser meros procedimentos de cópia de dados para se tornarem mecanismos imprescindíveis para que as organizações assegurem sua continuidade e, até mesmo, sobrevivência em um cenário de constantes ameaças cibernéticas, a exemplo dos cada vez mais frequentes ataques de *ransomware*[xxxi].

Atuação do CTIR Gov na coordenação da resposta aos ataques sofridos por órgãos públicos

212. Os ataques de novembro do ano passado ressaltaram a importância de os órgãos e entidades da Administração Pública se manterem articulados entre si, tanto para agilizarem a adoção de ações de remediação após a detecção de um incidente quanto para adotarem, de forma rápida e padronizada, ações preventivas e, assim, bloquearem outros ataques. Nesse sentido, destaca-se a atuação do CTIR Gov na coordenação da resposta aos ataques sofridos por diversos órgãos públicos.

213. Atuando em conjunto com a Secretaria de Governo Digital do Ministério da Economia (ME), a PF, o Serpro e a Dataprev, o CTIR Gov, durante o desenrolar do incidente, emitiu diversos alertas com vistas a atualizar os órgãos e entidades públicos sobre a campanha massiva de ataques de *ransomware* que estava em curso, bem como recomendar procedimentos e ações preventivas e corretivas[xxxii].

214. O último alerta relacionado a esse episódio consignou, por exemplo, que os ataques eram direcionados "aos sistemas VMware e Windows" e que se caracterizavam "por ações maliciosas para criptografar arquivos ou bancos de dados de instituições, a fim de exigir resgate em troca da

descriptografia dos arquivos cifrados"[xxxiii]. Assim, dentre as diversas informações e recomendações fornecidas, destacam-se as relativas às práticas de *backup*:

a) Que haja uma política de *backup* (cópia de segurança) definida;

b) Revisar as políticas de *backup* dos principais sistemas, executando testes em amostras para garantia de restauração;

c) Armazenar as cópias de segurança em local protegido, em rede exclusiva e isolada dos demais ativos, com acesso restrito e controlado por *Firewall*, com o devido registro de conexões;

d) Se possível, armazenar os *backups* em mais de um local físico, separados geograficamente, de preferência em cofres à prova de furto, incêndio e alagamento, com acesso controlado.

Comentários relevantes feitos pelos respondentes do questionário

215. Por meio da Questão 6.2, o questionário da auditoria oportunizou que os respondentes registrassem os principais desafios, deficiências e pontos de atenção relacionados à execução dos procedimentos de *backup* e *restore*, bem como outros comentários que considerassem pertinentes.

216. Com isso, foram coletadas 298 respostas que versaram, dentre outros assuntos, acerca da falta ou deficiência de recursos orçamentários e de pessoal de TI qualificado, bem como sobre a necessidade da implementação de melhorias na infraestrutura de TI. Quanto à carência de pessoal de TI e de recursos orçamentários, seguem alguns comentários registrados pelos respondentes:

No entanto o grande desafio é desenvolver os trabalhos necessários com a pouca mão de obra de servidores existente na área de TIC do Órgão.

O principal desafio é a falta de servidores capacitados para acompanhar as atividades técnicas. Os poucos servidores estão envolvidos em uma quantidade excessiva de contratos e planejamentos da contratação, restando pouco tempo para acompanhar a operação. Dessa forma, o órgão fica muito dependente dos profissionais da empresa contratada.

Inclusive, para o item de pessoal, o número de 7 (sete) servidores é insuficiente para as inúmeras demandas de Infraestrutura de TI do Órgão.

Esse baixo número de servidores efetivos e a carga de trabalho altíssima dificultam maiores esforços para a melhoria dos sistemas de *backup*, e, até mesmo, a capacitação dos servidores (...).

Recursos orçamentários e de recursos humanos para a área de TIC insuficientes.

Não há pessoal disponível para tratar especificamente e exclusivamente com *backup*. Os profissionais que executam essa tarefa são sobrecarregados com outras diversas atividades. (...) Além disso as restrições orçamentárias nos forçam a não investir melhor em *backup* (...).

217. A necessidade de melhoria da infraestrutura de TI – em especial para viabilizar os testes de *restore* – também foi muito apontada pelos respondentes, conforme ilustram os comentários a seguir:

O grande desafio em realizar as tarefas de cópias de segurança está relacionado principalmente a necessidade de estrutura para os testes de recuperação, pois, necessita-se para isso de pessoal, recursos de infraestrutura de processamento, de armazenamento, de licenças dentre outros, o que acarreta custos e mais especialização de pessoal.

Ampliação do ambiente de *backup* e *restore* que permita armazenar a integralidade de VM's e o teste periódico das cópias de *backup*.

O Instituto passou por um longo período sem investimentos na área de TI, inclusive de ferramentas de *backup* e suporte. Recentemente, foi realizado um pregão (...) para a aquisição de licenciamento e unidade de armazenamento em fita.

Obter a infraestrutura adequada (fitotecas) que permita atender as regras de "*backup* 3-2-1".

Quanto ao armazenamento remoto e *offline*, a principal deficiência encontrada é a de falta de recursos para implementar estas soluções (...). Quanto ao restauro de *backup*, a principal deficiência encontrada é a falta de recursos para aquisição de novos dispositivos de armazenamento mais rápidos para o *storage* principal (...).

Equipamentos de TIC obsoletos;

Não há ambiente adequado nem quantidade de servidores suficientes para estabelecer rotinas de teste de restauração dos *backups*.

Deficiência 1: Atualmente a instituição não possui um ambiente de redundância para *disaster recovery*. Deficiência 2: Os dados de *backup* (*appliance*) são armazenados no mesmo ambiente de produção.

218. No cenário atual, de grande complexidade do ambiente de TI em algumas organizações e de aumento significativo do volume de dados armazenados, alguns respondentes citaram a computação em nuvem como possível solução para replicação de dados e armazenamento de *backups* de forma remota:

> A adoção de uma solução de *backup* em nuvem ou a disponibilização de um *site* externo ao Tribunal para armazenamento de *backups* seria de grande valia para a organização.
>
> Principal desafio é ter recursos para ter os *backup's* em nuvem em sistema utilizado pela instituição.
>
> Realização de estudos para eventual adoção de *backup* em nuvem.
>
> Está em estudo a replicação de dados para ambiente remoto.
>
> Estão previstos a aquisição de solução de *storage* (em HD) e, futuramente, *backup* em nuvem (PaaS).
>
> Por questões de segurança, ainda não utilizamos solução de *backup* em nuvem.
>
> A Instituição está em processo de aquisição de repositório de *backup*; (...) Maior definição na política de *backup*, no sentido de verificar a viabilidade de *backup* em nuvem.
>
> Um grande desafio que se apresenta é o aumento do volume de dados a serem armazenados, em função das facilidades de utilização de arquivos de mídia que as ferramentas atualmente utilizam e que são mantidas armazenadas.
>
> Vale a pena ressaltar que a respeito do armazenamento em outro destino, há estudos para que possamos armazenar os dados seguindo as diretrizes adotadas do governo, em outro destino como a nuvem.
>
> (...) problema de espaço de armazenamento, ferramentas de *backup* mais modernas, fitas de *backup* perto do final da vida útil.
>
> O grande desafio nesse momento é conseguir ter uma única solução de *backup* que suporte todos os tipos de dados e sistemas, tendo em vista os custos de aquisição de tecnologia e a rápida obsolescência frente à velocidade que o volume de dados cresce.
>
> Falta de infraestrutura adequada para acomodação dos dois equipamentos de *backups* (*Datadomains*) em ambientes distintos e adequados.
>
> A gestão do *backup* das bases de dados do [sistema "X"] (...) tem se tornado cada vez mais complexa, devido ao seu crescimento acelerado. O tamanho do banco de dados já está em 58 TB. Isto compromete o rápido *restore* do banco.

219. Um desafio, não menos importante, apontado por um único respondente tratou da utilização de criptografia para proteger o *backup*:

> Aumentar a utilização de criptografia nos arquivos de cópia de segurança, de forma a proteger tais arquivos contra ameaças cibernéticas e acesso indevido.

220. Os respondentes também manifestaram preocupação com os custos da infraestrutura de TI:

> Alto custo na implantação, mas principalmente na manutenção de uma infraestrutura mais madura.
>
> Por fim, destacamos os elevados custos para a aquisição dos equipamentos necessários para ações de melhoria de *backup* dos dados como um todo. Temos um grande volume de dados armazenados que requerem não só equipamentos, mas também rede de dados de alto desempenho, compatível com a transferência desses dados de forma exequível.

221. Ademais, um respondente sugeriu incluir no questionário perguntas sobre "o tempo de vida da informação no *backup* e os meios de garantia da qualidade da informação".

222. E, pelo fato de o Serpro possuir diversos sistemas e bases de dados de alta relevância, o respectivo respondente sugeriu, de forma indireta, que o questionário não limitasse as respostas somente a um único sistema e/ou base de dados.

223. Por último, destaca-se que os comentários mostram já ser possível aferir benefícios advindos diretamente desta auditoria:

> A respeito da política de *backup*, informamos que o rascunho submetido como evidência foi criado em decorrência da auditoria em questão, reunindo as práticas e diretrizes atualmente em uso. Ela será trabalhada e formalizada como instrução normativa, após apreciação do Comitê Gestor de TI.
>
> Precisamos melhorar questões relacionadas a testes de *restore*, esse apontamento nesta auditoria forneceu insumos para incluir nas Ordens de Serviço rotineiras de cópias de segurança a partir do próximo mês de novembro os testes de *restore* e evidenciar para demonstrar que houve melhoria de processo.

224. Também nesse sentido, destaca-se que os comentários mostraram que os respondentes reconheceram a importância dos controles avaliados, bem como os benefícios trazidos pela auditoria ao se questionar a situação atual e induzir a movimentação de ações e projetos em curso ou planejados:

> 1. Estamos em processo de atualização da política de backup do órgão. (...) 4. Está em estudo a replicação de dados para ambiente remoto.
>
> Estão previstos a aquisição de solução de *storage* (em HD) e, futuramente, *backup* em nuvem (PaaS). Adicionalmente, estão sendo iniciados os trabalhos para implementarmos uma Política de *Backup*, alinhada à Política de Segurança de Informação, em processo de formalização (...).
>
> Apesar de termos política de *backup* que estabelece a realização de testes periódicos de recuperação (*restore*), essa norma não é seguida na prática, por não dispormos de hardware suficiente. (...) Já há previsão para revisão da política.
>
> Atualmente a instituição está planejando a política de *backup*, onde serão contemplados os procedimentos de teste e restauração dos *backups*.
>
> Estamos finalizando a criação das diretrizes com as orientações para a realização periódica dos testes de *restore*. O desafio neste momento é a implementação e execução dessas diretrizes.
>
> As oportunidades de melhoria sobre a temática são: instituição da política e plano de *backup*; realização dos testes de *restore*; armazenamento em sítio remoto; e a melhoria no controle de acesso físico às copias de segurança.
>
> O (...) deverá implantar espelhamento de dados em *site* remoto, com vistas a garantir alta disponibilidade para suas aplicações. Outrossim, construir um plano de *backup* formalizado e adotar o hábito de teste de *restore* de suas principais bases de dados.
>
> Os desafios são de conscientizar a alta gestão sobre a criticidade do tema e capacitar equipes de TI e *stakeholders* para construção de uma política institucional e plano de *backup* e *restore*.
>
> A Instituição está em processo de aquisição de repositório de *backup*; Necessidade de treinamento de equipe; Maior definição na política de *backup*, no sentido de verificar a viabilidade de *backup* em nuvem.
>
> Melhorar a documentação dos processos de trabalho referentes a *backup*/*restore* e criar plano de ação que nos torne mais aderentes às observações contidas nesta auditoria.
>
> A implementação de uma Política de *Backup* faz parte da estratégia de governança de TI do Ministério (...).
>
> A Política de *backup* está sendo reestruturada/revisada para melhor tratar as demandas do Ministério. A minuta inserida está em fase de revisão e será submetida à aprovação posteriormente.

É necessário formalizar uma política de *backup*, com definição clara dos dados necessários para cópia, periodicidade de armazenamento, local de armazenamento, testes de homologação e responsáveis pela execução e monitoramento do processo.

Pesquisa de avaliação da qualidade da fiscalização

225. Com o intuito de avaliar a qualidade da fiscalização, um segundo questionário foi utilizado para colher as opiniões dos respondentes relativamente à execução em si da auditoria. A Tabela 7 resume as 259 respostas a cada um dos oito questionamentos objetivos que foram feitos. Os seis primeiros possuíam apenas três opções de resposta ("Concordo", "Discordo" e "Não sei / Não se aplica"), enquanto os dois últimos tinham cinco ("Concordo totalmente", "Concordo em parte", "Discordo em parte", "Discordo totalmente" e "Não sei / Não se aplica").

**Tabela 7 - Resumo das respostas à pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

| Questionamento | Concordo / Concordo totalmente | Concordo em parte | Discordo em parte | Discordo / Discordo totalmente | Não sei / Não se aplica |
|---|---|---|---|---|---|
| Q1) Na comunicação de realização da auditoria, foram expostos, claramente, os objetivos do trabalho aos dirigentes da organização fiscalizada | 237 | - | - | 22 | - |
| Q2) As perguntas do questionário da auditoria foram bem formuladas (claras e objetivas), dispensando quaisquer esclarecimentos adicionais | 221 | - | - | 32 | 6 |
| Q3) A auditoria cumpriu seu propósito de expor à organização os riscos relacionados aos cinco subcontroles avaliados | 222 | - | - | 15 | 22 |
| Q4) A auditoria foi útil para a melhoria dos controles da organização | 214 | - | - | 20 | 25 |
| Q5) A auditoria resultou na implementação de ação específica no âmbito da organização | 157 | - | - | 59 | 43 |
| Q6) Caso o TCU disponibilize o questionário na forma de um serviço de autoavaliação, a organização teria interesse em preenchê-lo periodicamente, por conta própria | 192 | - | - | 22 | 45 |
| Q7) A metodologia utilizada | 133 | 94 | 9 | 1 | 22 |

| | | | | | |
|---|---|---|---|---|---|
| na auditoria (autoavaliação de controles) possui boa relação custo-benefício | | | | | |
| Q8) No geral, a organização está satisfeita com os resultados da auditoria | 114 | 100 | 16 | 1 | 28 |

226. Percebe-se que a grande maioria dos respondentes opinou de forma positiva quanto à qualidade da fiscalização, sendo que muitos comentaram que não avaliaram melhor (ou que marcaram a opção "Não sei / Não se aplica") por ainda não terem recebido retorno por parte do TCU a respeito de suas respostas ao questionário. Com relação a esses comentários, já foram elaborados os relatórios de *feedback* resultantes da auditoria (parágrafos 182-185), contendo as respostas de cada organização e incluindo sugestões de melhoria quanto aos seus procedimentos e comparações com as respostas das outras organizações auditadas. Esses relatórios serão enviados somente após autorização do Relator.

227. Uma oportunidade de melhoria apontada por muitos foi que, ao final do preenchimento do questionário, fosse oferecida ao respondente a oportunidade de salvar suas respostas, bem como de emitir alguma espécie de comprovante de conclusão. Também foi sugerido que o Tribunal enviasse as respostas para os e-mails dos respondentes. Esses procedimentos atenderiam a reclamação de um respondente no sentido de que o tempo entre as aplicações do questionário da auditoria e da posterior pesquisa de avaliação foi longo e que, portanto, ele já não se lembrava mais das respostas que havia fornecido.

228. Por outro lado, outros respondentes sugeriram que esse trabalho fosse realizado de forma periódica, sendo que um deles sugeriu que o instrumento utilizado fosse disponibilizado de forma permanente. Outro sugeriu a atribuição de uma nota que permitisse medir e acompanhar a evolução das organizações quanto à maturidade dos seus procedimentos de *backup* e *restore* – o que, de certo modo, já foi endereçado neste relatório por meio do indicador de qualidade (iBackup) descrito no bojo do Capítulo 4 (parágrafos 186-188).

229. Um respondente sugeriu que a metodologia utilizada nesta auditoria seja empregada em outros temas relacionados à TI. Também houve sugestão para que o questionário fosse mais abrangente, incluindo aspectos de continuidade do negócio e recuperação de desastres, dos quais os procedimentos de *backup* e *restore* são apenas alguns dos componentes. Outros sugeriram que a computação em nuvem fosse mais explorada no questionário, como opção à tradicional abordagem de *backup* em disco ou fita.

230. Vários respondentes sugeriram, ainda, que algumas questões fossem especificamente direcionadas à alta administração e às áreas de negócio, de modo a sensibilizar esses gestores para a importância do tema e ressaltar que a área de TI não é apenas "consumidora de recursos". Alguns reclamaram, novamente, da falta de recursos financeiros e de pessoal suficiente para aprimorar os processos da respectiva organização. Também foi sugerido que o resultado seja encaminhado ao dirigente máximo de cada organização, cobrando-se avanços. Um dos respondentes salientou, ainda, a importância do papel orientador, não apenas fiscalizador, desempenhado pelo TCU.

231. Considerando que um dos respondentes reclamou que o Tribunal não informou sobre o acesso, o uso e a guarda dos dados informados, destaca-se que a tela inicial do questionário registrou:

> 3) Por poderem conter informações sensíveis, as evidências (*upload* de arquivos) enviadas no âmbito desta auditoria serão consideradas, de antemão, classificadas como reservadas, nos termos do art. 23, inciso I, c/c art. 24, § 1º, inciso III, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI).

232. Destaca-se que as respostas ao terceiro questionamento (Tabela 7, Q3) mostraram que a grande maioria concordou que a auditoria cumpriu efetivamente o seu propósito de expor às organizações auditadas os riscos relativos aos cinco subcontroles avaliados (Figura 28).

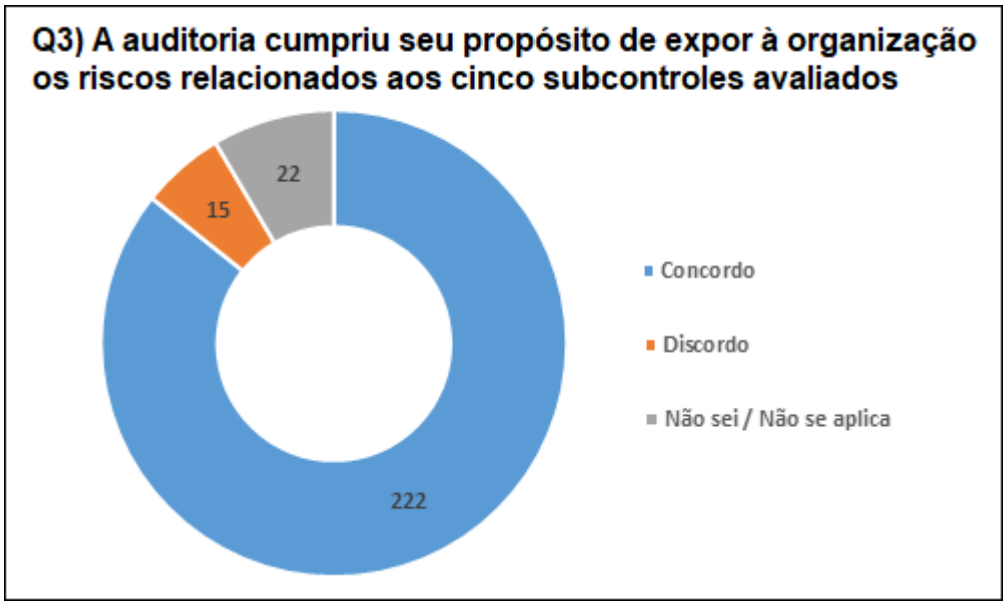


**Figura 28 - Distribuição das respostas à Q3 da pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

233. Por sua vez, as respostas ao quarto questionamento (Tabela 7, Q4) mostraram que a auditoria foi útil para a melhoria dos controles da grande maioria das organizações participantes (Figura 29)

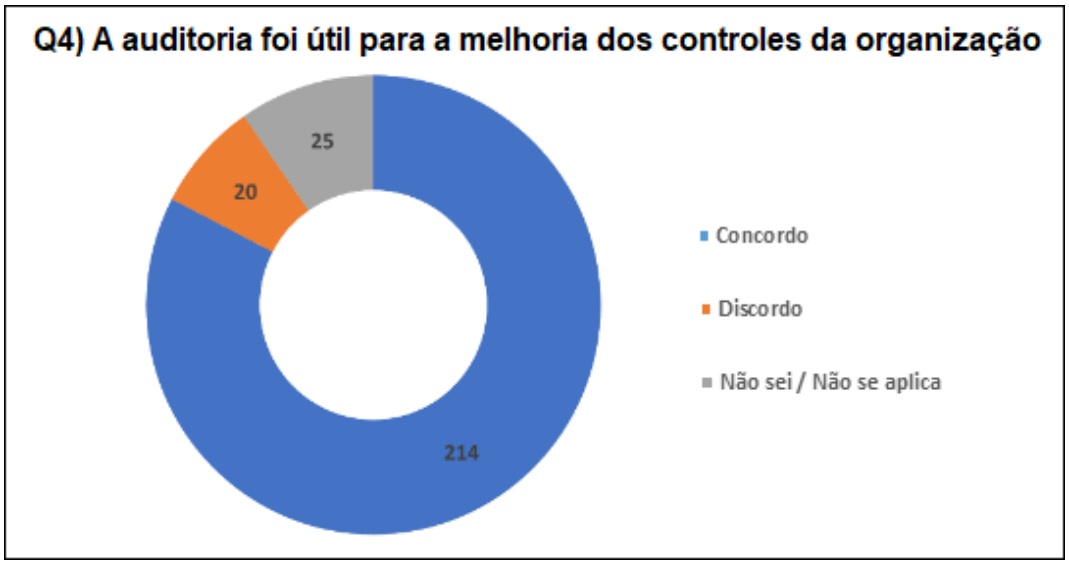


**Figura 29 - Distribuição das respostas à Q4 da pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

234. Como benefício imediato, destaca-se, ainda, que as respostas ao quinto questionamento (Tabela 7, Q5) mostraram que, em 157 das organizações, a auditoria já resultou na implementação de ações específicas (Figura 30).

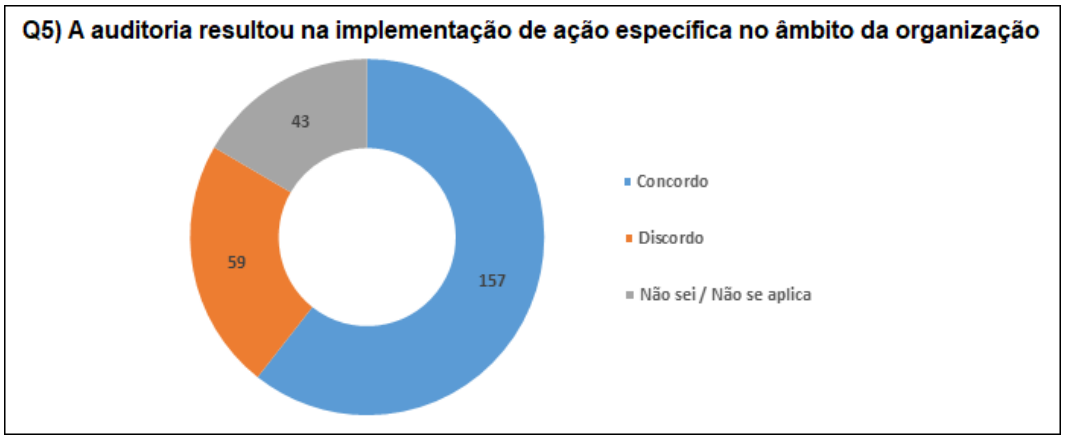


**Figura 30 - Distribuição das respostas à Q5 da pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

235. Destacam-se os comentários de um respondente no sentido de que a auditoria ajudou "a identificar algumas fragilidades na nossa infraestrutura e serviu de guia para elaboração de alguns documentos, também nos motivou a planejar o desenvolvimento de um serviço que atenda ao controle nº 10 (Data Recovery Capabilities) do Framework do CIS" e que foi determinado "como foco para 2021, o fortalecimento e implementação de políticas voltadas para continuidade dos serviços de TIC e segurança da informação (Gerenciamento de incidentes, backup etc.)". Outro informou que, "diante da provocação do TCU", a empresa está em fase de criação de uma política de *backup* unificada, a ser aplicada em toda a sua rede. Outro comentou, ainda, que a auditoria foi importante para obter o patrocínio da alta administração da organização.

236. As respostas ao sexto questionamento (Tabela 7, Q6) mostraram que 192 dos respondentes teria interesse em preencher o questionário da auditoria periodicamente, por conta própria, caso o TCU venha a disponibilizá-lo na forma de um serviço de autoavaliação (Figura 31).

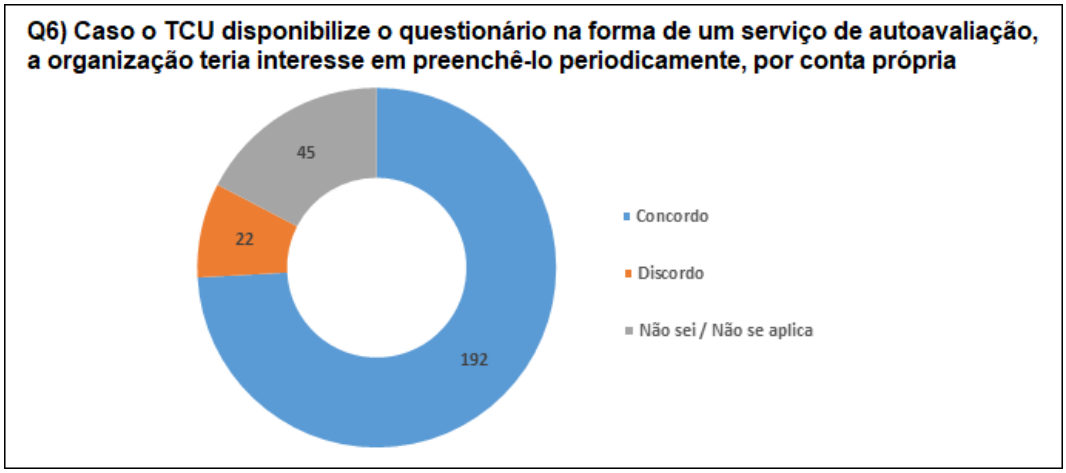


**Figura 31 - Distribuição das respostas à Q6 da pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

237. De modo geral, os respondentes concordaram (totalmente ou em parte) que a metodologia CSA, utilizada na auditoria, apresenta boa relação custo-benefício (Tabela 7, Q7 - Figura 32).

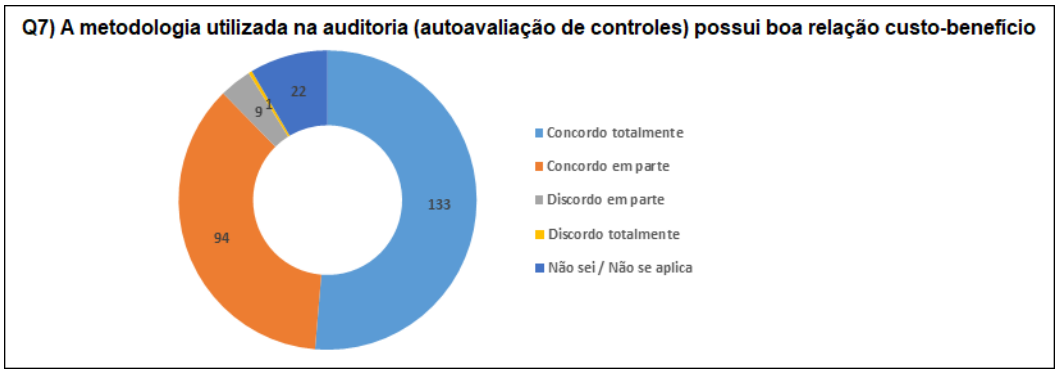


**Figura 32 - Distribuição das respostas à Q7 da pesquisa de avaliação da qualidade da fiscalização.**
(Fonte: elaboração própria, com base nas respostas à pesquisa de avaliação da qualidade da fiscalização)

238. Um respondente, que discordou em parte dessa afirmação, comentou que trabalhos baseados em questionários abordam, em sua maioria, aspectos quantitativos e/ou de simples confirmação e que, portanto, uma boa relação custo-benefício só seria obtida por meio de uma avaliação na auditoria "se o que estamos fazendo, a forma como é feita e as ferramentas utilizadas estão de acordo com o mercado ou mesmo com a natureza da atividade da empresa". Outro, a seu turno, ponderou excessivo o tempo gasto para o preenchimento do questionário da auditoria e comentou que, de modo geral, essa avaliação é importante, porém que a considera "extremamente burocratizada e dispendiosa para as empresas".

239. No entanto, diante do conjunto dos comentários fornecidos pelos respondentes, a equipe da fiscalização entendeu que a avaliação acerca da relação custo-benefício da metodologia utilizada (autoavaliação de controles por parte do próprio gestor) restou parcialmente prejudicada, tendo em vista ainda não ter havido o retorno, por parte do TCU, a respeito dos dados coletados, o que só acontecerá com o encaminhamento dos relatórios de *feedback* e do acórdão decorrente da auditoria às organizações.

## 7. Perspectiva para o futuro

240. No relatório do levantamento da governança e gestão de segurança da informação e de segurança cibernética da APF, finalizado recentemente pelo TCU (TC 001.873/2020-2; Acórdão 4.035/2020-TCU-Plenário; Rel. Min. Vital do Rêgo), a Sefti propôs, dentre outras ações no âmbito da Estratégia de Fiscalização do TCU em SegInfo e SegCiber, a realização de um acompanhamento ágil de controles críticos de SegCiber (Figura 24, Eixo "Diagnosticar").

241. Esse acompanhamento envolveria a realização, por parte dos próprios gestores, de autoavaliações de controles (metodologia CSA – parágrafos 11-12) construídas com base nos vinte controles de SegCiber preconizados pelo CIS (Tabela 1), alinhadas à aplicação da metodologia ágil de gerenciamento de projetos. A ideia inicial seria, então, aplicar às organizações da APF uma sequência de vinte questionários (correspondendo àqueles vinte controles), tratando cada aplicação como uma *sprint* consecutiva. Eventualmente, a quantidade dessas *sprints* poderia ser reduzida, caso a equipe considerasse conveniente agrupar dois ou mais controles em um único questionário.

242. Esta auditoria sobre procedimentos de *backup* pode ser considerada uma espécie de "piloto" daquele acompanhamento, com a avaliação de um único controle (10 – Capacidades de recuperação de dados), precipitada em face do alto risco de ataques de *ransomware*, conforme mapeado pela Sefti[3,18,19].

243. Assim, a Sefti ainda pretende continuar avaliando os demais controles críticos do *framework* do CIS. Porém, a partir da experiência adquirida com esta fiscalização, dois aspectos da ideia original foram alterados: i) não devem ser verificados, necessariamente, todos os vinte controles do CIS, tampouco todos os subcontroles relativos a cada um desses controles; e ii) não deve ser seguida a ordem numérica dos vinte controles para a condução dessas verificações.

244. Ou seja, esta unidade técnica realizará um trabalho de priorização para definir os próximos controles a serem auditados, os quais poderão ser agrupados, tanto em termos dos controles em si quanto dos seus subcontroles componentes. A propósito, o próprio CIS recomenda que as organizações priorizem a implementação desses controles e subcontroles levando em consideração seus respectivos portes e suas "expertises" em SegCiber.

245. Adicionalmente, as organizações auditadas poderão ser filtradas com base em critérios de relevância, materialidade e risco, consequentemente reduzindo-se o número total de questionários a serem aplicados. Esse processo de enxugamento, inclusive, já teve início na auditoria conduzida para avaliar aspectos relacionados à implementação da LGPD nas organizações da APF (TC 039.606/2020-1; Rel. Min. Augusto Nardes)[xxxiv].

246. Assim, sugere-se que a fiscalização desses controles prossiga em processo apartado do tipo acompanhamento, voltado à contínua obtenção de dados e realização de análises (RI/TCU, arts. 241 e 242, em especial o inciso II), no bojo do qual as organizações da APF seriam continuamente avaliadas por meio de múltiplos questionários, a serem oportunamente construídos e aplicados aos gestores. A próxima verificação, por exemplo, poderá envolver, conjuntamente, os dois primeiros controles básicos (Inventário e controle de ativos de hardware e de software), cuja implementação possibilita que a organização gerencie seus dispositivos de hardware e software conectados em rede, de modo a permitir apenas a utilização de ativos autorizados, detectando e bloqueando, automaticamente, quaisquer outros.

247. Outra avaliação poderá aferir a maturidade quanto ao controle 3 (Gerenciamento contínuo de vulnerabilidades), cuja finalidade é reduzir a janela de oportunidade disponível para a exploração de vulnerabilidades por eventuais atacantes, visto que, muitas vezes, o sucesso de um ataque pode decorrer, justamente, de haver um lapso de tempo excessivo entre a descoberta e a correção de determinada falha.

248. Além desses três controles "básicos", poderá ser verificado, na sequência, um dos controles "organizacionais", a exemplo do 19 – Resposta e gerenciamento de incidentes, cuja temática já recebeu, inclusive, proposta de ação de fiscalização na Estratégia de Fiscalização do TCU em SegInfo e SegCiber (Figura 24, Eixo "Diagnosticar"). Segundo o CIS, esse controle busca assegurar que a organização defina uma infraestrutura de resposta a incidentes capaz de, rapidamente, detectar eventuais ataques, conter os danos, erradicar a presença do invasor e restaurar a integridade da sua rede, dados e sistemas.

249. A priorização dessa verificação no processo de resposta a incidentes cibernéticos das organizações decorre, principalmente, de duas razões. A primeira foi apontada no citado relatório (parágrafo 240), que propôs a realização dessa fiscalização ao concluir que "relativamente aos riscos e vulnerabilidades em SegInfo/SegCiber, o cenário encontrado merece atenção, especialmente quanto à real capacidade da APF para responder e tratar incidentes de SegInfo, por parte de cada órgão individualmente e da rede de ETIRs por eles formada" (TC 001.873/2020-2, peça 46, parágrafo 511).

250. A segunda, a seu turno, resulta da aprovação da LGPD, que trouxe os "planos de resposta a incidentes e remediação" como parte do "programa de governança em privacidade" a ser implementado no âmbito das organizações (Lei 13.709/2018, art. 50, § 2º, inciso I, alínea "g").

251. Por último, destaca-se que, após realizadas pela primeira vez, essas verificações dos controles críticos de SegCiber preconizados pelo CIS devem ser repetidas periodicamente, de modo a permitir que o TCU seja capaz de identificar o grau e a velocidade da evolução da maturidade das organizações nessa seara, com o passar do tempo.

## 8. Conclusão

252. Esta auditoria objetivou avaliar se os procedimentos de *backup* e *restore* das organizações da APF, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados.

253. Com esse propósito, e tomando por base os cinco subcontroles do décimo controle crítico de SegCiber (*Data Recovery Capabilities*) do *framework* preconizado pelo CIS, foi construído e

disponibilizado um questionário *online* para ser respondido por gestores de 422 organizações da APF, o qual obteve um total de 410 (97,2%) respostas. As perguntas feitas, então, buscavam jogar luz sobre cinco macroquestões, relacionadas aos referidos subcontroles (parágrafos 7.1-7.5).

254. A partir das análises das respostas e evidências fornecidas pelas organizações no âmbito do questionário, condensadas no Capítulo 2, foi possível obter um panorama geral nessa área, de modo a responder, efetivamente, as cinco questões elaboradas no planejamento da auditoria, além de outras.

255. De início, considera-se alarmante o fato de que 74,6% das organizações respondentes (306 de 410) não possuem política de *backup* aprovada formalmente, pois trata-se do documento básico, negociado entre as áreas de negócio ("dona" dos dados/sistemas) e de TI da organização, com vistas a disciplinar as questões e procedimentos relacionados à execução das cópias de segurança (*backups*), a exemplo do escopo dos dados (bases de dados, sistemas de arquivos, imagens de servidores etc.) a serem copiados, suas respectivas periodicidades (diária, semanal, mensal etc.), tipos (completo/*full*, diferencial, incremental), quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança (controle de acesso, localização remota, criptografia etc.).

256. Relativamente à execução de *backups* da principal base de dados da organização, o cenário encontrado surpreendeu positivamente, com 99,2% (373 de 376) das organizações que afirmaram tratar diretamente alguma base de dados efetuando *backups* completos com alguma periodicidade e, dessas, 94,9% (354 de 373) o fazendo de forma automatizada, de acordo com os preceitos do subcontrole 10.1 (*Ensure Regular Automated Backups*) do *framework* do CIS.

257. No que tange aos *backups* do principal sistema, considera-se preocupante que, das organizações que disseram hospedar sistemas em servidores/máquinas próprios, 71,2% (265 de 372) não possuem plano de *backup* específico para seu principal sistema. Percebe-se como positivo, no entanto, que 84,4% (314 de 372) dessas organizações realizem cópias ao menos semanais do seu principal sistema e que, de todas as organizações que executam essas cópias (mesmo mensal ou apenas ocasionalmente), 60,8% (206 de 339) o fazem de forma integral (*e.g.* cópia da imagem das máquinas), em sintonia com os ditames do subcontrole 10.2 (*Perform Complete System Backups*) do mesmo *framework*.

258. A seu turno, também merece atenção a constatação de que mais da metade das organizações respondentes (216 de 410: 52,7%) registrou não executar quaisquer testes de restauração (*restore*) dos seus *backups*, aliada ao fato de que, mesmo entre aquelas que afirmaram realizar tais testes, 59,8% (116 de 194) não os documentam. Como consequência, há risco de que, em situações reais em que seja preciso recuperar um sistema e/ou dados da organização a partir das cópias armazenadas, isso não seja efetivamente possível, tornando sem utilidade todo o processo de *backup*/*restore* da organização, ao contrário do que preconiza o subcontrole 10.3 (*Test Data on Backup Media*) do citado *framework*.

259. Quanto à proteção dos *backups*, a auditoria identificou duas vulnerabilidades principais. A primeira é que dois terços das organizações que afirmaram realizar *backups* (254 de 385: 66%), apesar de implementarem mecanismos de controle de acesso físico ao local de armazenamento desses arquivos, não os armazenam criptografados, o que acarreta risco de vazamento de dados da organização, que pode causar enormes prejuízos, sobretudo se envolver informações sensíveis e/ou sigilosas. A segunda desconformidade consiste na ausência de registro dos acessos ao ambiente segregado onde os *backups* são armazenados por parte de 51,4% (179 de 348) das organizações que mantêm local próprio para isso.

260. Ou seja, percebe-se que as organizações ainda têm muito a evoluir em relação às práticas do subcontrole 10.4 (*Protect Backups*) do *framework* do CIS, ressaltando-se que, atualmente, implementar rotinas criptográficas sobre os arquivos dos *backups* não é algo complexo, pode ser configurado para ocorrer de forma automática na maioria das ferramentas e atua para prevenir que a organização incorra em penalidades em virtude de descumprimentos relacionados à LGPD.

261. Por último, também foi verificado que 60,2% das organizações respondentes (247 de 410) não mantêm suas cópias em ao menos um destino não acessível remotamente, o que não atende aos preceitos do subcontrole 10.5 (*Ensure All Backups Have at Least One Offline Backup Destination*) e acarreta risco de que, em um ataque cibernético (de *ransomware*, por exemplo), os próprios arquivos dos *backups* acabem sendo corrompidos, excluídos e/ou criptografados pelo atacante ou *malware*, tornando igualmente sem efeito o processo de *backup*/*restore* da organização.

262. As fragilidades detectadas (sintetizadas no Anexo V - Matriz de achados), de modo geral, decorrem de falta de maturidade nas organizações (possivelmente causada por uma série de razões, tais como orçamento insuficiente para a área de TI, carência quantitativa e qualitativa de pessoal, ausência de capacitações e treinamentos, falta de apoio da alta administração etc.), conforme mostrado por meio da identificação de correlação positiva entre a maturidade das organizações em gestão de SegInfo e a adoção das boas práticas de *backup*/*restore* avaliadas nesta auditoria (iBackup – Figuras 26 e 27).

263. De modo a contribuir para o cenário encontrado, esta equipe proporá a edição de normativos específicos para orientar os gestores e regulamentar a obrigatoriedade de que as organizações públicas aprovem formalmente e mantenham atualizadas políticas e planos de *backup* (para seus sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os aspectos abordados neste relatório.

264. Frisa-se que, como a fiscalização teve por propósito conscientizar e orientar os gestores respondentes quanto aos riscos relativos à ausência/deficiência dos subcontroles questionados no âmbito deste trabalho, envolvendo, inclusive, a elaboração de relatórios de *feedback* às organizações auditadas (Capítulo 4), entende-se que, mesmo antes da edição das referidas normas, as organizações devem se organizar para suprir essas falhas, sob pena de passarem por situações similares àquelas enfrentadas pelos órgãos que sofreram ataques cibernéticos recentes (Capítulo 6).

265. Adicionalmente, as organizações podem se preparar para serem novamente auditadas em relação aos seus controles de *backup*/*restore*, bem como aos demais controles críticos de SegCiber do CIS, priorizando a implementação daqueles explicitamente mencionados no Capítulo 7.

## 9. Propostas de encaminhamento

266. Diante do exposto, submetem-se os autos à consideração do Relator, Ministro Vital do Rêgo, com as seguintes propostas:

266.1. determinar a autuação de processo apartado, do tipo acompanhamento (RI/TCU, arts. 241 e 242), com vistas a dar continuidade à avaliação dos controles críticos de segurança cibernética no âmbito dos órgãos e entidades da Administração Pública federal, como consequência natural desta auditoria e em linha com a Estratégia de Fiscalização do TCU em Segurança da Informação (SegInfo) e Segurança Cibernética (SegCiber), sugerida no TC 001.873/2020-2;

266.2. recomendar ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP), com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de *backup* (para suas bases de dados e sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (*Data Recovery Capabilities*) do *framework* preconizado pelo *Center for Internet Security* (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança;

266.3. nos termos do art. 8º da Resolução - TCU 315/2020, fazer constar, na ata da sessão em que estes autos forem apreciados, comunicação do relator ao colegiado no sentido de monitorar a recomendação contida no item anterior;

266.4. encaminhar cópias eletrônicas deste relatório e do acórdão decorrente desta fiscalização, bem como do relatório e do voto que fundamentarem este último, ao GSI/PR, ao CNJ e ao CNMP, bem como às organizações públicas auditadas;

266.5. autorizar a Secretaria de Fiscalização de Tecnologia da Informação, observada eventual necessidade de despersonificação e de reserva quanto a questões específicas, a dar ampla divulgação às informações e aos produtos derivados da execução desta auditoria, em especial à ficha-síntese e aos relatórios de *feedback*, a fim de alavancar a maturidade das organizações da APF relativamente à gestão dos seus procedimentos e rotinas de *backup* e *restore*, com reflexos nas respectivas resiliências quanto a falhas de segurança, vulnerabilidades e ataques cibernéticos;

266.6. arquivar o presente processo, com fulcro no art. 169, inciso V, do RI/TCU."

É o relatório.

---

[i] BRASIL. Tribunal de Contas da União (TCU). Boletim do TCU (BTCU) Especial - Ano 39, nº 1 (2/1/2020). *Regimento Interno do Tribunal de Contas da União (Republicado)*. Brasília: TCU, 2020, 85p. Disponível em: <https://portal.tcu.gov.br/data/files/2A/C1/CC/6A/5C66F610A6B96FE6E18818A8/BTCU_01_de_02_01_2020_Especial%20-%20Regimento_Interno.pdf>. Acesso em 24/3/2021.

[ii] BRASIL. Tribunal de Contas da União (TCU). Boletim do TCU (BTCU) Especial - Ano 39, nº 29 (12/11/2020). *Portaria - Segecex nº 18, de 12 de novembro de 2020*. Brasília: TCU, 2020, 111p. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/btcu/*/NUMEROBTCU%253A29%2520ANOBTCU%253A2020/DTRELEVANCIA%2520desc/0>. Acesso em 24/3/2021.

[iii] BRASIL. Tribunal de Contas da União (TCU). Boletim do TCU (BTCU) nº 75/2020. *Resolução - TCU nº 315, de 22 de abril de 2020*. Brasília: TCU, 2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/ato-normativo/*/TIPO%253A%2528Resolu%25C3%25A7%25C3%25A3o%2529%2520NUMATO%253A315%2520NUMANOATO%253A2020/score%2520desc/0>. Acesso em 24/3/2021.

[iv] BRASIL. Tribunal de Contas da União (TCU). *Acórdão 4.035/2020-TCU-Plenário*. Relator: Ministro Vital do Rêgo. Brasília: TCU, 8/12/2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A4035%2520ANOACORDAO%253A2020/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0>. Acesso em 24/3/2021.

[v] BRASIL. Tribunal de Contas da União (TCU). *Acórdão 2.737/2020-TCU-Plenário*. Relator: Ministro-Substituto Marcos Bemquerer em substituição ao Ministro Vital do Rêgo. Brasília: TCU, 14 de outubro de 2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A2737%2520ANOACORDAO%253A2020/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0>. Acesso em 24/3/2021.

[vi] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/001.873%252F2020-2>. Acesso em 24/3/2021.

[vii] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/ato-normativo/*/TIPO:%22Portaria%22%20NUMATO:280%20NUMANOATO:2010/DTRELEVANCIA%20desc,NUMATOINT%20desc/0>. Acesso em 24/3/2021.

[viii] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/ato-normativo/*/TIPO:%22Portaria%22%20NUMATO:168%20NUMANOATO:2011/DTRELEVANCIA%20desc,NUMATO%20desc/0>. Acesso em 24/3/2021.

[ix] Organização Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). Comitê de Normas Profissionais. *ISSAI 100 – Princípios Fundamentais de Auditoria do Setor Público*. Copenhague: 2013, 17p. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A2561DF3F501562345D11B534C>. Acesso em 24/3/2021.

[x] Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles>. Acesso em 24/3/2021.

[xi] Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/auditoria-sobre-backup>. Acesso em 24/3/2021.

[xii] Disponível em: <https://www.cisecurity.org/controls/cis-controls-list>. Acesso em 24/3/2021.

[xiii] Disponível em: <https://pt.wikipedia.org/wiki/Ransomware>. Acesso em 24/3/2021.

[xiv] Disp. em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527>. Acesso em 24/3/2021.

[xv] Disponível em: <https://tiinside.com.br/15/10/2020/brasileiros-sao-alvo-de-quase-metade-dos-ataques-de-ransomware-na-america-latina>. Acesso em 24/3/2021.

[xvi] Disponível em: <https://www.controle.net/faq/tipos-de-backup-o-que-e-backup-full-incremental-e-diferencial>. Acesso em 24/3/2021.

[xvii] Disponível em: <https://cartilha.cert.br/fasciculos/backup/fasciculo-backup.pdf>. Acesso em 24/3/2021.

[xviii] Disponível em: <https://tiinside.com.br/18/03/2021/pesquisa-58-dos-backups-de-dados-estao-falhando> e <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=56438&sid=97>. Acesso em 24/3/2021.

[xix] Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=19/03/2018&jornal=515&pagina=22&totalArquivos=134>. Acesso em 24/3/2021.

[xx] Disponível em: <https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=16/07/2014&jornal=1&pagina=5&totalArquivos=84>. Acesso em 24/3/2021.

[xxi] BRASIL. Associação Brasileira de Normas Técnicas (ABNT). *NBR ISO/IEC 27002: Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação*. Rio de Janeiro: ABNT, 2013, 99p.

[xxii] Disponível em: <https://veja.abril.com.br/blog/radar-economico/brasil-sofre-seu-maior-ataque-hacker-da-historia>, <https://www.securityreport.com.br/destaques/especialistas-comentam-onda-de-ciberataque-em-orgaos-do-governo>, <https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema>, <https://olhardigital.com.br/2020/11/12/seguranca/hacker-invade-sistema-da-cgu-e-divulga-passo-a-passo-da-acao-no-youtube>, <https://www.cisoadvisor.com.br/grupo-hacker-invade-servidor-do-cnj-e-alega-ter-consertado-falha>, <https://noticias.uol.com.br/politica/ultimas-noticias/2020/11/05/apos-stj-hackers-paralisam-sistemas-do-ministerio-da-saude-e-governo-do-df.htm>, <https://www.cisoadvisor.com.br/ransomware-publica-208-gb-de-dados-do-conselho-federal-de-contabilidade>, <https://www.correiobraziliense.com.br/brasil/2020/11/4886902-rede-do-ministerio-da-saude-esta-fora-do-ar-e-suspeita-e-de-ataque-de-hackers.html>, <https://g1.globo.com/df/distrito-federal/noticia/2020/11/05/governo-do-df-tira-sistemas-online-do-ar-apos-ataque-hacker.ghtml>, <https://g1.globo.com/es/espirito-santo/noticia/2020/11/09/servicos-on-line-da-prefeitura-de-vitoria-ficam-indisponiveis-apos-ataque-hacker.ghtml>, <https://www.agazeta.com.br/es/cotidiano/nao-ha-previsao-de-retorno-do-servico-digital-em-vitoria-diz-secretario-1120> e <https://www.agazeta.com.br/es/cotidiano/ataque-hacker-em-vitoria-10-dias-depois-nem-todos-os-servicos-voltaram-1120>. Acesso em 24/3/2021.

[xxiii] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 24/3/2021.

[xxiv] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Em-razao-de-ataque-cibernetico--STJ-funcionara-em-regime-de-plantao-ate-o-dia-9.aspx>. Acesso em 24/3/2021.

[xxv] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/04112020-Ministerio-da-Justica-encaminha-oficio-do-STJ-a-PF-para-abertura-de-inquerito.aspx>. Acesso em 24/3/2021.

[xxvi] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/05112020-Em-regime-de-plantao-ate-restabelecimento-da-rede--STJ-analisa-pedidos-urgentes.aspx>. Acesso em 24/3/2021.

[xxvii] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/08112020-Comunicado-da-Presidencia-do-STJ.aspx>, <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09112020-Comunicado-da-Presidencia-do-STJ.aspx>, <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/10112020-Comunicado-da-Presidencia-do-STJ.aspx>, <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/11112020-Comunicado-da-Presidencia-do-STJ.aspx> e <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 24/3/2021.

[xxviii] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/07112020-Comunicado-da-Presidencia-do-STJ.aspx>, <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/16112020-Comunicado-da-Presidencia-do-STJ.aspx> e <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/18112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 24/3/2021.

[xxix] Disponível em: <https://tiinside.com.br/12/11/2020/sofisticacao-do-ataque-ao-stj-assustou>, <https://www.cisoadvisor.com.br/stj-mais-de-1200-servidores-congelados-backups-destruidos>, <https://obastidor.com.br/justica/hacker-cobra-resgate-de-dados-sequestrados-do-stj-26>, <https://backupgarantido.com.br/blog/superior-tribunal-de-justica-stj-foi-alvo-de-ataque-de-ransomware-sistema-ainda-esta-fora-do-ar> e <https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack>. Acesso em 24/3/2021.

[xxx] Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/06112020-Comunicado-da-Presidencia-do-STJ.aspx>, <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/14112020-Comunicado-da-Presidencia-do-STJ.aspx> e <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/15112020-Comunicado-da-Presidencia-do-STJ.aspx>. Acesso em 24/3/2021.

[xxxi] Disponível em: <https://olhardigital.com.br/2020/12/31/noticias/ransomware-pode-se-tornar-um-problema-ainda-maior-em-2021>. Acesso em 24/3/2021.

[xxxii] Disponível em: <https://www.ctir.gov.br/alertas>. Acesso em 24/3/2021.

[xxxiii] Disponível em: <https://www.ctir.gov.br/arquivos/alertas/2020/alerta_especial_2020_07_atualizacao_ataques_de_ransomware.pdf>. Acesso em 24/3/2021.

[xxxiv] Disponível em: <https://portal.tcu.gov.br/imprensa/noticias/auditoria-do-tcu-vai-avaliar-a-adequacao-das-organizacoes-publicas-a-lgpd.htm>. Acesso em 24/3/2021.

# VOTO

Em exame, relatório de auditoria realizada no período de outubro de 2020 a abril de 2021, com vistas a avaliar a efetividade dos procedimentos de *backup* das organizações públicas federais. Foram consultadas 422 organizações federais no trabalho. As informações coligidas foram analisadas por treze unidades técnicas do TCU sob a coordenação da Secretaria de Fiscalização de Tecnologia da Informação (Sefti).

## II

2. O ano de 2020, sob os efeitos da pandemia de Covid-19, também ficou conhecido pela aceleração da revolução digital. Desde a chegada da internet, o mundo passava por progressiva e veloz adoção de tecnologias. Contudo, os riscos à saúde pública e as restrições de contato e de convívio social que se impuseram em razão da pandemia catalisaram esse processo, consolidando o mundo digital como palco central de significativas mudanças comportamentais.

3. A administração pública que, por sua vez, já vinha passando por sucessiva digitalização dos serviços públicos, viu-se, repentinamente, sob a necessidade de incorporar em larga escala novas rotinas e procedimentos para manter-se funcionando. Com isso, o meio digital passou não somente a ser o principal meio de prestação de serviços à sociedade, mas também o ambiente de trabalho principal de grande parte dos agentes públicos. Assim, tribunais passaram a se reunir virtualmente, departamentos inteiros começaram a se reunir virtualmente, viagens foram reduzidas, interações entre servidores migraram para os softwares e o acesso remoto a arquivos e sistemas corporativos deixou a condição de exceção e passou a ser a regra.

4. Com efeito, a segurança das informações e o fortalecimento da segurança cibernética, que já eram temas extremamente relevantes para a preservação dos serviços públicos, ganhou novo relevo após as mudanças econômicas e sociais trazidas pela pandemia.

5. Já em meio ao novo contexto, em dezembro de 2020, tive a oportunidade de trazer à consideração do Plenário no âmbito do TC 001.873/2020-2, levantamento realizado pelo TCU com o objetivo de conhecer a macroestrutura de governança e gestão de segurança da informação e de segurança cibernética da Administração Pública Federal, incluindo aspectos acerca da legislação, políticas, normativos, atores, papéis e responsabilidades atinentes àquelas áreas. O trabalho resultou no Acórdão 4.035/2020-TCU-Plenário.

6. Naquela ocasião, o setor público enfrentava grave ataque à sua infraestrutura de tecnologia da informação. Um dos órgãos mais afetados, o Superior Tribunal de Justiça (STJ), teve seus serviços completamente paralisados por vários dias em função do ataque perpetrado contra seu ambiente de informação.

7. Segundo informações obtidas pela unidade técnica, o STJ considerou ter sofrido "o pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade". A resposta ao episódio teria mobilizado "mais de 50 servidores do [seu] quadro permanente", contou com o suporte e o apoio técnico de "oito fabricantes de tecnologia (hardware e software)" e envolveu a colaboração da Polícia Federal (PF), do Comando de Defesa Cibernética (ComDCiber) do Exército Brasileiro e do Serviço Federal de Processamento de Dados (Serpro) na investigação.

8. O STJ não era, entretanto, o único órgão atingido. As atividades criminosas causaram indisponibilidade de serviços de TI em órgãos como Conselho Nacional de Justiça (CNJ), Controladoria-Geral da União (CGU), Ministério da Saúde (MS), Governo do Distrito Federal (GDF) e Conselho Federal de Contabilidade (CFC), entre outros.

9. Desde então, e a partir daquele levantamento de cenário, esta Corte de Contas não se manteve inerte, tendo iniciado este trabalho com vistas a avaliar e a fomentar adoção de práticas de backup voltadas à maior proteção das informações. E o cenário mostra que tal decisão foi acertada. Por ocasião da apreciação deste trabalho, o Poder Judiciário foi alvo de novo ataque hacker. De acordo com matérias divulgadas na mídiai em 30/4/2021, o Tribunal de Justiça do Rio Grande do Sul foi objeto de um ataque do tipo ransomware, modalidade em que os dados dos sistemas são criptografados e seu acesso completamente bloqueado por invasores. Segundo se noticiou, os cibercriminosos solicitam U$ 5 milhões para desbloquear os sistemas daquela corte.

10. Tal cenário de materialização de riscos vem sendo objeto de atuação desta Casa há muito tempo, diga-se de passagem. Há decisões do TCU acerca do assunto há mais de vinte anos. Posso citar a Decisão 445/1998-Plenário, de Relatoria do Min. Carlos Átila, em que o Plenário decidiu determinar à Caixa Econômica, na condição de agente operador do FGTS que:

> 3.7. adote, quanto à segurança e confiabilidade dos sistemas de processamento de dados empregados na operacionalização do FGTS, as seguintes providências:
> (...)
> 3.7.2. definir, oficialmente, junto aos gestores responsáveis, uma sistemática de "back-up" para os sistemas existentes;

11. Em outra ocasião, recordo que, no âmbito de ampla fiscalização para avaliar os sistemas integrados de gestão, mais conhecidos como sistemas ERP, o TCU emitiu recomendações a empresas estatais para que aumentassem a proteção sobre suas cópias de segurança. Como exemplo, menciono o Acórdão 2.296/2012-TCU-Plenário, de relatoria do Min. Walton Alencar, em que o TCU identificou fragilidades e fez recomendações à Casa da Moeda do Brasil:

> 310. A norma existente (2012-NA-1-02) que trata da geração de cópias de segurança e recuperação de dados na CMB é superficial e está desatualizada. Há documento infranormativo que descreve alguns procedimentos de backup (peça 44, p. 4-13), porém este, além de incompleto, não está formalizado. Não há detalhamento dos procedimentos de recuperação de dados, nem previsão de realização periódica de testes desses procedimentos e das mídias utilizadas para backup (itens 303 a 306). (...)
>
> 9.2.20. elabore, aprove formalmente e dê ampla divulgação a uma política de cópias de segurança, de acordo com as recomendações do item 10.5 da NBR ISO/IEC 27002:2005, e à semelhança das orientações do objetivo de controle DS11.5 do Cobit 4.1;

12. O tema, portanto, é objeto de alertas desta Corte de Contas há anos e, com o passar do tempo, o volume de informações e a criticidade dos sistemas que gerenciam essas bases de dados somente cresceu.

13. De acordo com informações do portal do governo digital brasileiro, o Gov.br, o número de serviços digitais oferecidos pelo governo saltou de 737 em 2017 para 2.424 serviços em 2020, sendo que 62% dessa quantia eram considerados pelo governo como totalmente digitais. Desde então o número não parou de crescer. Atualmente, o portal do governo divulga que estão disponíveis online 3.909 serviços de 190 órgãos da administração pública.

14. Os riscos decorrentes de falhas na gestão da segurança da informação são de toda ordem e podem representar desde problemas relacionados à integridade de dados públicos e pessoais, passando pelo vazamento de informações sigilosas, confidenciais e pessoais, bem como podendo provocar impactos econômicos negativos em caso de indisponibilidade de serviços ou falhas em sistemas e bases de dados.

15. Portanto, em um contexto de maior digitalização e maior risco às informações e à disponibilidade dos serviços públicos, a adoção de processos adequados para conferir preservação e proteção a dados e serviços é fator de primeira importância.

16. Além do trabalho que relatei, recordo que, por ocasião do julgamento do Acórdão 1.889/2020-TCU-Plenário, o voto do relator, Ministro Aroldo Cedraz, trouxe a conhecimento informações mais detalhadas de levantamento que procurou identificar e definir os chamados "sistemas críticos" da administração pública, ou seja, aqueles sistemas cujas falhas têm potencial de causar impactos severos sobre a operação das organizações públicas e a prestação de serviços aos cidadãos de uma forma geral.

17. Naquele trabalho, registrou-se que cerca de 77,4% dos sistemas considerados críticos estavam armazenados em centros de dados próprios, ou seja, de gestão individual de uma organização pública, enquanto pouco mais de 20% estavam armazenados em datacenters de terceiros, estruturas normalmente mais robustas e com mais controles de segurança da informação, a exemplo dos datacenters das empresas públicas de serviços de TI, notadamente Serpro e Dataprev.

18. Chamo a atenção para esse número, pois, conforme se verá adiante, as fragilidades identificadas nos controles de muitas organizações públicas apontam para estruturas e processos deficitários em termos de segurança e proteção e dados.

19. Cabe lembrar que os riscos à segurança da informação e à segurança cibernética, requerem controles de diferentes ordens, envolvendo dispositivos físicos, lógicos, organizacionais, processos, cultura, dentre outros.

20. O Center for Internet Security (CIS), organização não governamental com forte atuação na área, tem reconhecimento internacional por seus códigos de boas práticas (frameworks) em segurança de sistemas e dados, em particular, o CIS Controls. O framework CIS é composto por vinte controles considerados críticos para a segurança na internet. Entre os controles apontados encontram-se a produção de inventários, o uso controlado de privilégios administrativos, o gerenciamento contínuo de vulnerabilidades, as defesas contra malware, os programas de conscientização e treinamento em segurança e, o objeto do presente estudo, as capacidades de recuperação de dados.

21. No framework, esse controle é subdividido em outros cinco subcontroles, que versam sobre a realização de cópias de segurança, testes de restauração, armazenamento e proteção das cópias de segurança.

22. Assim, a presente fiscalização teve por objetivo verificar a capacidade das organizações públicas federais de executar com consistência procedimentos de cópias de segurança (backups) e de recuperação de dados (restore), em especial sobre bases de dados e sistemas críticos.

23. Para tanto, nessa fiscalização utilizou-se a autoavaliação de controles internos, metodologia chamada de CSA (control self-assessment), tendo sido disponibilizado aos gestores públicos um questionário para que eles próprios respondessem acerca das práticas organizacionais com relação aos controles de backup/restore implementados, anexando-se a documentação comprobatória.

24. A fiscalização foi então estruturada em torno de cinco questões de auditoria, cada uma contendo um grupo de perguntas específicas no questionário aplicado. Eis as questões:

Q1) A organização realiza, de forma regular e automática, cópias de segurança (backups) da sua principal base de dados?

Q2) A organização realiza, regularmente, cópias de segurança (backups) integrais (e.g. cópia da imagem) dos servidores/máquinas que hospedam seu principal sistema?

Q3) A organização realiza, periodicamente, testes de restauração (*restore*) das cópias de segurança (backups) citadas nas questões anteriores?

Q4) A organização implementa mecanismos de controle de acesso físico (e.g. sala cofre) e lógico (e.g. criptografia) para proteger as cópias de segurança (backups)?

Q5) A organização armazena as cópias de segurança (backups) em ao menos um destino não accessível remotamente?

25. Em uma fiscalização com aplicação típica da metodologia CSA, a auditoria atua como facilitadora do processo, apoiando e coordenando o preenchimento do instrumento de coleta, analisando resultados e apresentando devolutivas (informação de feedback) com vistas a permitir que cada organização seja capaz de planejar e implementar as melhorias que considerar mais relevantes e de acordo com sua realidade.

III

26. Feita essa breve contextualização, apresento a seguir a síntese dos principais achados e as respectivas conclusões e encaminhamentos acerca dos temas avaliados nesta auditoria.

27. Uma política de backup (ou instrumento normativo equivalente) consiste, de maneira resumida, em um acordo de alto nível entre as áreas de negócio e de TI da organização para consignar as regras quanto aos backups de dados da organização, qual a periodicidade, tipos de backup, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança.

28. O primeiro achado registrado no relatório refere-se à inexistência de política de geração de cópias de segurança (backup e restore) aprovada formalmente na organização. Apesar de se tratar de um controle básico, aproximadamente metade das organizações respondentes (208 de 410: 50,7%) ainda não possuem tal documento e, das 202 que o elaboraram, quase metade (98 de 202: 48,5%) não a formalizaram.

29. A inexistência de política de backup leva à indefinição em relação ao escopo dos dados (bases de dados, sistemas de arquivos etc.) que deverão ser copiados, periodicidade (diária, semanal, mensal), quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos que podem representar riscos à segurança das informações.

30. Por outro lado, o segundo e o terceiro achado da fiscalização foram considerados positivos.

31. O segundo diz respeito à regularidade de realização do procedimento de cópias. Segundo verificou a auditoria, as cópias de segurança (backups) da principal base de dados da organização são realizadas de forma regular e automática. Das organizações consultadas que afirmaram tratar diretamente alguma base de dados (376 organizações), 99,2% (373 organizações) executam backups completos dessa base com periodicidade, sendo que 45,9% (171 de 373) fazem cópias diariamente ou mais de uma vez por dia. A execução periódica de cópias diminui o risco de perda de dados, uma vez que permite a recuperação dos dados em caso de falhas.

32. O terceiro achado, também considerado positivo, constatou que cópias de segurança (backups) integrais (e.g. cópia da imagem das máquinas) do principal sistema da organização são realizadas regularmente. Segundo se apurou, de 372 organizações que afirmaram hospedar sistemas em servidores/máquinas próprios, mais de 75% realizam esses backups diariamente, sendo que 84,4% realizam pelo menos semanalmente.

33. Contudo, cumpre-me destacar uma informação negativa existente no relato desse achado, 33 organizações públicas (8,9% do total) informaram que não realizam backup de seu principal sistema, colocando-se em situação de total vulnerabilidade a falhas e ataques, o que é simplesmente inconcebível.

34. Nesse mesmo sentido, o quarto achado destacou a Inexistência de plano de backup específico para o principal sistema da organização, dado que mais de 70% das organizações (71,2%) informaram não adotar esse controle mesmo em se tratando de seu principal sistema. Em que pese tais organizações possam estar realizando cópias de segurança que protejam seu principal sistema, a inexistência do plano acarreta indefinição em relação ao escopo dos dados a serem copiados, periodicidades, locais de armazenamento, tempo de retenção necessário, entre outros requisitos de

segurança, que podem estar em descompasso com os requisitos de negócio.

35. Avanço agora para o próximo ponto: a falta de testes dos backups efetuados.

36. É necessário frisar: um backup que não funciona não tem utilidade. Pior, pode gerar uma falsa sensação de segurança. Em função disso, as boas práticas recomendam que as cópias de segurança sejam regularmente testadas para certificar-se de sua utilidade. Tais testes, conhecidos como testes de restauração, destinam-se a simular o processo de recuperação de informações em caso de um incidente, de modo a assegurar que, sempre que necessário, a recuperação de sistemas e bases de dados da organização a partir das cópias de segurança seja possível.

37. Apesar da relevância, o quinto achado – a organização não realiza ou não documenta os testes de restauração (restore) das suas cópias de segurança (backups) – foi identificado para a maioria das organizações (52,7%). E mesmo da parte que realiza esses testes, quase metade o faz somente em relação aos backups da sua principal base de dados (46,9%), sendo que a maioria (59,8%) não os documenta.

38. Essa situação expõe a elevado risco grande parte das organizações públicas. Segundo informações obtidas pela equipe de auditoria, uma pesquisa realizada com três mil tomadores de decisões em empresas globais informou que cerca de 58% dos backups realizados apresentam falhas, o que, consequentemente, tem o potencial de deixar as informações desprotegidas. Assim, a falta de testes periódicos sobre as cópias de segurança não colabora para a mitigação dos riscos a que estão expostas as organizações públicas.

39. Ainda que as cópias sejam feitas e testadas com regularidade, há outros riscos que precisam ser mitigados, como o de vazamento de informações a partir das cópias de segurança.

40. Muitas vezes, os sistemas estão submetidos a severos controles de segurança, porém não é incomum que o mesmo rigor não se aplique às cópias de segurança efetuadas.

41. De acordo com a auditoria, o sexto achado, a organização não protege adequadamente suas cópias de segurança (backups), foi identificado em dois terços das organizações, ou seja, 66% não armazenam os arquivos de maneira criptografada, medida considerada básica para resguardar sua confidencialidade e evitar vazamentos de dados.

42. Ainda, cerca de 20% das organizações utilizam solução intermediária, em que a criptografia só é aplicada no servidor de backup ou na nuvem, ou seja, os arquivos de backup trafegam pelas redes de maneira desprotegida. Na verdade, apenas 14% das organizações (54 de 385) afirmaram utilizar a tecnologia de "criptografia de ponta-a-ponta", evitando que os dados trafeguem de maneira desprotegida nas redes.

43. Por fim, o sétimo e último achado - A organização não armazena suas cópias de segurança (backups) em ao menos um destino não acessível remotamente – registrou que mais da metade das organizações (60,2%, ou 247 de 410) não mantém seus backups em ao menos um destino não acessível remotamente. Tal medida é importante para minimizar o risco de que os próprios arquivos de backup sejam alvo de ataques criminosos, especialmente os temidos ataques de ransomware.

## IV

44. Diante das constatações, verifico que ainda há baixa maturidade das organizações públicas no que diz respeito à realização de cópias de segurança. Recordo que, consoante a metodologia CSA, as observações foram obtidas a partir das informações preenchidas pelas próprias organizações. Com efeito, há risco não desprezível de que a situação pudesse se mostrar ainda mais vulnerável caso os critérios de verificação e fiscalização fossem mais rigorosos.

45. O minucioso relatório apresentado pela Secretaria de Fiscalização de TI apresenta ainda

painel de consulta interativa para permitir maiores análises sobre as informações obtidas. Outrossim, a partir dos dados coletados, elaborou-se um indicador, denominado iBackup, para permitir comparações entre as organizações auditadas no que tange à qualidade geral dos procedimentos de backup/restore.

46. Segundo apurou a equipe, há correlação positiva entre os estágios de maturidade em gestão de segurança da informação e a adoção de boas práticas de backup/restore avaliadas na fiscalização.

47. Instados a se manifestar sobre os desafios, deficiências e pontos de atenção relacionados à execução dos procedimentos de backup e de restore, os gestores produziram 298 respostas, as quais trouxeram menções de falta ou deficiência de recursos orçamentários e de pessoal qualificado, bem como sobre necessidade de implantação de melhorias na infraestrutura de TI.

48. Sobre esse prisma, cumpre-me retomar o início deste voto, e acrescentar reflexões àquelas já manifestadas pela unidade técnica.

49. Embora os desafios enfrentados por organizações públicas e suas áreas técnicas sejam reais, entendo que a solução não passa unicamente pelo aumento dos investimentos. Há quase quinze anos o Tribunal acompanha, por meio de unidade especializada, a situação do setor de tecnologia da informação na administração pública federal, e a carência de recursos humanos e orçamentários sempre seguiu sendo apontada como causa de problemas.

50. Inclusive, em pesquisa destinada a avaliar a própria qualidade da presente fiscalização, respondentes sugeriram que questões fossem direcionadas à alta administração, com o fito de sensibilizar administradores para a importância do tema com o fito de que pudessem constatar a falta de recursos financeiros e de pessoal suficiente para aprimorar os processos da organização.

51. Não obstante as pertinentes manifestações técnicas dos respondentes, cumpre-me dissentir parcialmente e tecer acréscimos às soluções aventadas.

52. Compreendo que, mais uma vez, agora sob a ótica da segurança, verificam-se os efeitos negativos da fragmentação, da duplicação e da verticalização presente na TI pública, que se estendem além da descentralização razoável e necessária.

53. Em outras palavras, a administração pública não dispõe, e provavelmente jamais irá dispor, de recursos suficientes para dotar individualmente cada organização pública de numerosa equipe de TI, com alta qualificação e com recursos orçamentários e infraestrutura individual compatível com suas necessidades. Ouso dizer que, inclusive, seria ineficiente.

54. Essa preocupação não é desconhecida do Tribunal, que já se debruçou a analisar o modelo de operação de tecnologia da informação do Poder Executivo Federal. Por oportuno, trago à baila, excertos do Relatório que fundamentou o Acórdão 2.789/2019-TCU-Plenário, de relatoria do Min. Raimundo Carreiro:

> 30. Em conjunto, as organizações integrantes do Sisp empenharam aproximadamente R$ 6,5 bilhões em despesas de TI no ano de 2017, segundo dados do Siop, o que representou 1,7% do orçamento total dos órgãos fiscalizados. Importante notar que apenas 26 órgãos respondem por 80% deste gasto, o que demonstra, por um lado, uma grande fragmentação em pequenas unidades de TI e, por outro lado, uma grande concentração do orçamento em poucos órgãos de maior relevância. (...)
>
> 65. A fragmentação da TI em múltiplas organizações não é um problema em si, pois traz vantagens operacionais. É útil quando há muita diversidade de áreas finalísticas e favorece que se atenda mais rapidamente às necessidades locais. No entanto, carrega dificuldades que são inerentes à sua natureza: duplicação de funções, custos maiores, compartimentalização de conhecimento e menor alinhamento com a estratégia geral. Sem dúvida, estas dificuldades podem ser superadas, porém outros fatores presentes na realidade da APF as potencializam, em detrimento das vantagens mencionadas.

> 66. Nesse sentido, a verticalização das operações contribui sobremaneira para a ampliação dos problemas inerentes a um modelo fragmentado de TI. Ela significa que cada organização de TI é uma cópia dos seus pares, responsável por executar toda a pilha de serviços que compõem uma operação de TI: infraestrutura básica, redes e telecomunicações, software básico, middleware, sistemas administrativos, sistemas de negócio, sistemas de apoio à decisão, portais, etc., inclusive no que diz respeito aos processos de aquisição e sustentação do seu ambiente computacional. Isto impõe às organizações a necessidade de desenvolver suas capacidades por completo, e à Administração Pública como um todo, a necessidade de dispender mais recursos para custear suas operações.
>
> 67. À semelhança da fragmentação, a verticalização não é um problema em si mesma, não fosse a conjugação de dois outros fatores: a falta de padronização das tecnologias utilizadas pela APF e a limitação de pessoal a que todo o governo está submetido. A falta de padronização das tecnologias afeta o acúmulo de conhecimento e a disseminação de boas práticas, o que poderia reduzir as necessidades de capacitação de pessoal e tornar a troca de experiências e movimentação de pessoal mais eficiente. Além disso, diminui a possibilidade de o Estado tirar proveito do efeito escala como grande comprador de tecnologia, aumentando a pressão sobre os custos. (...)
>
> 188. É preciso salientar, também, que a **fragmentação da infraestrutura de TI pode promover um aumento dos riscos operacionais a que as organizações estão expostas**. Se, por um lado, a multiplicidade de *datacenters* divide os riscos de falhas comprometerem um grande número de serviços simultaneamente, por outro lado a **maior necessidade de prover recursos humanos e financeiros para manter todas as múltiplas instalações atualizadas, em termos de vida útil dos equipamentos, de confiabilidade e de segurança da informação, restringida ainda por contingenciamentos orçamentários, expõe os órgãos a um nível de risco maior de falhas**. (...) (grifou-se).

55. Portanto, percebidos de forma individual, é natural que muitas organizações não tenham capacidades e recursos para dotar seus sistemas e bases de dados de controles suficientes para a proteção das informações e sistemas organizacionais. Não se pode admitir que organizações públicas sem as menores condições técnicas e orçamentárias de manter complexos centros de dados, devam prover toda a cadeia de serviços de uma infraestrutura de TI típica.

56. A situação, pede, portanto, novas estratégias, que propiciem maiores ganhos de escala sobre a segurança e a proteção dos dados públicos.

57. Os próprios gestores apontam a computação em nuvem como possível solução para replicação de dados e armazenamento de backups de forma remota. Fundamenta-se na percepção que o compartilhamento de infraestruturas, processos e recursos e humanos é fundamental para a melhora da situação. A continuarmos presos a modelos de informatização que preconizaram a excessiva verticalização de unidades de tecnologia da informação, as quais muitas vezes não dispõem de recursos para fazer o básico, a administração seguirá vulnerável a ataques cada vez mais danosos e significativos à sua infraestrutura.

58. Ao contrário, iniciativas transversais como a construção do portal Gov.br, que veio substituir centenas de portais individuais de organizações públicas, mostram que o caminho passa por uma associação mais inteligente de descentralização, porém com compartilhamento de estruturas, processos e pessoas.

59. Observo que, tais iniciativas, constam da Estratégia de Governo Digital (EGD) para o período de 2020 a 2022, estabelecida por meio do Decreto 10.332/2020. Entre os objetivos ligados à otimização das infraestruturas de TI, destaco as iniciativas 16.4 - Otimizar a infraestrutura de, pelo menos, trinta datacenters do Governo federal, até 2022 e 16.5 - Migração de serviços de, pelo menos, trinta órgãos para a nuvem, até 2022.

60. Portanto, em acréscimo às propostas formuladas pela unidade técnica, voto para que seja

dada ciência do presente trabalho à Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República, unidade responsável por coordenar a execução da Estratégia de Governo Digital.

V

61. Feitas essas constatações, adoto como minhas razões de decidir os fundamentos presentes no relatório de fiscalização naquilo que não colidirem com as demais manifestações realizadas ao longo deste voto.

62. Enquanto o compartilhamento e o provimento transversal de infraestrutura não for realidade para muitas organizações públicas, e com o múnus de preservação das informações e dos serviços públicos, reputo pertinentes as deliberações sugeridas pela fiscalização.

63. Portanto, acompanho a proposta da unidade técnica, com as devidas alterações de forma, de recomendar aos órgãos responsáveis a edição de normativos e regulamentações para orientar e dispor acerca da obrigatoriedade de formalizar políticas gerais e adotar controles necessários e sugeridos pelas boas práticas.

64. Tendo em vista o resultado positivo obtido com a realização da presente fiscalização, a qual representou uma espécie de piloto, ao analisar um dos controles críticos de segurança cibernética, a unidade técnica propõe que seja dado seguimento ao trabalho de avaliação de tais controles, mediante processo de acompanhamento, como consequência natural desta fiscalização. Dessa feita, acolho a proposta formulada, sem prejuízo de determinar à Sefti que, previamente ao início de cada etapa do acompanhamento, submeta ao Relator o processo contemplando o escopo da respectiva etapa da fiscalização.

65. Espera-se que as recomendações que estão sendo propostas possam contribuir para o aumento de segurança sobre os sistemas e informações públicos, bem como espera-se que a próxima fiscalização prevista possibilite acompanhar a implementação de controles críticos de segurança cibernética, de forma a criar um ciclo positivo de amadurecimento da gestão de segurança da informação.

Com essas considerações, voto para que seja adotada a minuta de acórdão que ora trago à apreciação deste colegiado.

TCU, Sala das Sessões Ministro Luciano Brandão Alves de Souza, em 12 de maio de 2021.

Ministro VITAL DO RÊGO
Relator

[i] https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADcia/sites-revelam-que-cibercriminosos-querem-u-5-milh%C3%B5es-para-desbloquear-sistema-informatizado-do-tjrs-1.612125

ACÓRDÃO Nº 1109/2021 – TCU – Plenário

1. Processo TC 036.620/2020-3.
2. Grupo I – Classe de Assunto: V – Auditoria.
3. Responsável: não há.
4. Entidades: várias.
5. Relator: Ministro Vital do Rêgo.
6. Representante do Ministério Público: Subprocurador-Geral Paulo Bugarin.
7. Unidade Técnica: Secretaria de Fiscalização de Tecnologia da Informação (Sefti).
8. Representação legal: não há.

9. Acórdão:

VISTOS, relatados e discutidos estes autos de auditoria com vistas a avaliar a efetividade dos procedimentos de backup das organizações públicas federais;

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em Sessão do Plenário, ante as razões expostas pelo Relator, em:

9.1 recomendar ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP), com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de *backup* (para suas bases de dados e sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (*Data Recovery Capabilities*) do *framework* preconizado pelo *Center for Internet Security* (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança;

9.2. informar da presente decisão à Secretaria Executiva do Gabinete de Segurança Institucional da Presidência da República, ao Conselho Nacional de Justiça, ao Conselho Nacional do Ministério Público, à Secretaria Especial de Modernização do Estado da Secretaria-Geral da Presidência da República, bem como às demais organizações públicas auditadas;

9.3. autorizar a Secretaria de Fiscalização de Tecnologia da Informação:

9.3.1 a encaminhar a cada instituição fiscalizada o seu respectivo relatório de feedback de modo a permitir o desenvolvimento de ações de melhoria na gestão da segurança da informação;

9.3.2. em conjunto com a Segecex, observada eventual necessidade de despersonificação e de reserva quanto a questões específicas, a dar ampla divulgação a informações agregadas e consolidadas nos produtos derivados da execução desta auditoria, a fim de alavancar os esforços de adoção de boas práticas e de cumprimento de normas de segurança da informação e de segurança cibernética pelos órgãos da APF;

9.4 retornar os autos Secretaria de Fiscalização de Tecnologia da Informação para que ela promova a autuação de processo apartado do tipo acompanhamento, com fundamento nos art. 241 e 242 do Regimento Interno deste Tribunal e nos termos do art. 24, parágrafo único, da Resolução-TCU 175/2005, com vistas a dar continuidade à avaliação dos controles críticos de segurança cibernética no âmbito dos órgãos e entidades da Administração Pública federal, e consoante o disposto no levantamento que resultou no Acórdão 4.035/2020-TCU-Plenário;

9.5. arquivar o presente processo, com fulcro no art. 169, inciso V, do RI/TCU.

10. Ata n° 16/2021 – Plenário.
11. Data da Sessão: 12/5/2021 – Telepresencial.
12. Código eletrônico para localização na página do TCU na Internet: AC-1109-16/21-P.

13. Especificação do quórum:
13.1. Ministros presentes: Ana Arraes (Presidente), Walton Alencar Rodrigues, Benjamin Zymler, Augusto Nardes, Aroldo Cedraz, Raimundo Carreiro, Vital do Rêgo (Relator) e Jorge Oliveira.
13.2. Ministro-Substituto convocado: Augusto Sherman Cavalcanti.
13.3. Ministros-Substitutos presentes: Marcos Bemquerer Costa, André Luís de Carvalho e Weder de Oliveira.

(Assinado Eletronicamente)
ANA ARRAES
Presidente

(Assinado Eletronicamente)
VITAL DO RÊGO
Relator

Fui presente:

(Assinado Eletronicamente)
CRISTINA MACHADO DA COSTA E SILVA
Procuradora-Geral