GRUPO tagGrupo – CLASSE V – tagColegiado
TC 036.301/2021-3 [Apensos: TC 000.284/2022-0 e 000.372/2022-6].
Natureza(s): Relatório de Acompanhamento.
Entidades: vários.
Interessados: Câmara dos Deputados (00.530.352/0001-59); Secretaria de Governo Digital do Ministério da Economia.
Representação legal: não há

**SUMÁRIO: AUDITORIA DE ACOMPANHAMENTO. MAPEAMENTO DA MATURIDADE DAS ORGANIZAÇÕES PÚBLICAS FEDERAIS QUANTO À IMPLEMENTAÇÃO DE CONTROLES CRÍTICOS DE SEGURANÇA CIBERNÉTICA (SEGCIBER). FRAGILIDADES NA ADOÇÃO DE CONTROLES E NA PROTEÇÃO DE SERVIÇOS E INFORMAÇÕES. RECOMENDAÇÕES. AÇÕES PEDAGÓGICAS E NORMATIVAS. ANÁLISE INCIDENTE CIBERNÉTICO NO MINISTÉRIO DA SAÚDE (INVASÃO HACKER COM INTERRUPÇÃO DE SERVIÇOS DE SAÚDE). DESAPENSAMENTO. DETERMINAÇÃO. CONSTITUIÇÃO DE ACOMPANHAMENTO EM APARTADO PARA ACOMPANHAMENTO DOS DESDOBRAMENTOS DO INCIDENTE NA SAÚDE.**

## RELATÓRIO

Adoto como relatório a instrução de mérito elaborada no âmbito da Secretaria de Fiscalização de Tecnologia da Informação - Sefti (peça 855), que contou com parecer favorável da chefia imediata (peça 856) e da unidade técnica (peça 857), a seguir transcrita no essencial:

> "Trata-se de fiscalização do tipo acompanhamento, conforme previsto nos arts. 241 e 242 do Regimento Interno do Tribunal de Contas da União (RI/TCU)[i] e no art. 24, parágrafo único, da Resolução - TCU 175/2005[ii], conduzida de acordo com o "Manual de Acompanhamento"[iii]. Para a expedição das propostas de encaminhamento, foi observada a Resolução - TCU 315/2020[iv].
>
> 1.1. Decisão que originou a fiscalização
>
> 2. No âmbito da "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023"**Error! Bookmark not defined.**, foi prevista a realização, em 2021, de um "Acompanhamento de controles críticos de SegCiber" (Figura 39, eixo "Diagnosticar").
>
> 3. Essa fiscalização, então, foi autorizada por meio do item 9.4 do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria para avaliar a efetividade dos procedimentos de *backup*/*restore* das organizações públicas federais; Rel. Min. Vital do Rêgo)**Error! Bookmark not defined.**. Em seu voto, o Relator consignou:
>
> > Tendo em vista o resultado positivo obtido com a realização da presente fiscalização [auditoria de *backup*/*restore* dos órgãos e entidades da APF], 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. (grifo nosso)

4. Assim, em 30/8/2021, foi submetido ao Relator documento apresentando a visão geral e o escopo específico deste primeiro ciclo do acompanhamento (peça 4), tendo o Relator, em despacho de 9/9/2021, manifestado sua ciência e anuído, então, com o início da realização da fiscalização (peça 7).

1.2. Identificação do objeto

5. Gestão de controles críticos de SegCiber das organizações públicas federais.

1.3. Objetivo e escopo do acompanhamento

6. O objetivo do trabalho é contribuir para o esforço de TD das organizações públicas, conscientizando os gestores das áreas de SegInfo acerca dos riscos aos quais suas organizações estão sujeitas em virtude de incidentes e ataques cibernéticos, de modo que estes implementem, ao longo dos próximos anos, medidas de segurança e controles adequados para endereçar esses riscos.

7. Para isso, neste primeiro ciclo do acompanhamento, foram verificadas as vinte medidas de segurança básicas (IG1) que fazem parte dos cinco controles a seguir (ver Tabela 1):

7.1. 1) Inventário e controle de ativos corporativos: medidas 1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos; e 1.2 - Tratar ativos não autorizados.

7.2. 2) Inventário e controle de ativos de software: medidas 2.1 - Estabelecer e manter um inventário de software; 2.2 - Assegurar que o software autorizado seja atualmente suportado; e 2.3 - Tratar softwares não autorizados.

7.3. 7) Gestão contínua de vulnerabilidades: medidas 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidades; 7.2 - Estabelecer e manter um processo de correção de vulnerabilidades; 7.3 - Executar a gestão automatizada de correções (*patches*) de sistemas operacionais; e 7.4 - Executar a gestão automatizada de correções (*patches*) de aplicativos.

7.4. 14) Conscientização sobre segurança e treinamento de competências: medidas 14.1 - Estabelecer e manter um programa de conscientização em segurança; 14.2 - Treinar os colaboradores para reconhecerem ataques de engenharia social; 14.3 - Treinar os colaboradores em melhores práticas de autenticação de usuários; 14.4 - Treinar os colaboradores em melhores práticas de tratamento de dados; 14.5 - Treinar os colaboradores para evitarem exposição não intencional de dados; 14.6 - Treinar os colaboradores para reconhecerem e notificarem incidentes de segurança; 14.7 - Treinar os colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos; e 14.8 - Treinar os colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras.

7.5. 17) Gestão de respostas a incidentes: medidas 17.1 - Designar responsáveis por gerenciar o tratamento de incidentes; 17.2 - Estabelecer e manter informações de contato para reporte de incidentes de segurança; e 17.3 - Estabelecer e manter um processo para o recebimento de notificações de incidentes.

8. Para melhor exposição do conteúdo, o Capítulo 2 apresenta os resultados gerais para cada uma das perguntas relacionadas a esses controles, individualmente (a íntegra do questionário *online* aplicado às 377 organizações públicas federais encontra-se no Anexo I da peça 855), enquanto o Capítulo 3 traz os principais "registros" derivados desses resultados. A Matriz de Planejamento pode ser conferida no Anexo II da peça 855**Error! Reference source not found.**.

1.4. Processos conexos

9. O TC 031.436/2019-6 (Rel. Min. Aroldo Cedraz)[v] consistiu em levantamento com vistas a identificar os sistemas informacionais críticos da APF (os quais precisam ter sua segurança reforçada) e elaborar diagnóstico da capacidade de fiscalização das unidades técnicas do Tribunal

com foco nesses sistemas[vi], tendo resultado na elaboração da "Estratégia de Fiscalização de Sistemas Críticos – EFISC".

10.O TC 001.873/2020-2 (Rel. Min. Vital do Rêgo)[vii] tratou de levantamento da governança e gestão de SegInfo/SegCiber da APF, em cujo relatório foi proposta a "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023", que previu, entre suas ações, a condução deste acompanhamento.

11.A seu turno, o TC 036.620/2020-3 (Rel. Min. Vital do Rêgo)[viii] consistiu em auditoria realizada sobre a efetividade dos procedimentos de *backup*/*restore* das organizações públicas federais, fiscalização que serviu como piloto para testar a adequabilidade da aplicação do método de autoavaliação de controles internos (CSA) para verificar um controle crítico de SegCiber (a capacidade de recuperação de dados é tratada no controle 11 do *framework* do CIS), tendo resultado no Acórdão 1.109/2021-TCU-Plenário, cujo item 9.4 autorizou, então, a autuação deste acompanhamento.

12.Por fim, o TC 039.606/2020-1 (Rel. Min. Augusto Nardes)[ix] foi um trabalho de auditoria com o objetivo de avaliar os riscos à proteção de dados pessoais e os consequentes preparo e conformidade das organizações públicas federais em relação às exigências da Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)[x], bem como a estruturação da Autoridade Nacional de Proteção de Dados (ANPD). Até esta data, os autos ainda não foram julgados.

## 1.5. Métodos utilizados

13.O trabalho foi conduzido em conformidade com as Normas de Auditoria do TCU – NAT (Portaria - TCU 280/2010[xi], alterada pela Portaria - TCU 168/2011[xii]) e com o Manual de Acompanhamento[iii] e está alinhado aos Princípios Fundamentais de Auditoria do Setor Público, conforme tradução da ISSAI 100, disponibilizada pelo portal do TCU[xiii].

14.A metodologia utilizada (CSA) 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.

15.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[xiv].

16.O acompanhamento foi construído tomando por base as 153 medidas de segurança previstas nos dezoito controles críticos de SegCiber da versão 8 do *framework* do CIS (Tabela 1, peça 855**Error! Reference source not found.**), a serem gradativamente verificadas ao longo de sete ciclos de execução (Tabela 2, peça 855).

17.É importante salientar que, apesar de esse *framework* poder ser considerado, ele próprio, um padrão de boas práticas amplamente reconhecido e utilizado, no Brasil e no mundo, por gerentes e auditores de TI, também há critérios normativos que dão suporte aos controles e às medidas de segurança avaliadas, a exemplo da Instrução Normativa (IN) GSI/PR 3/2021 (gestão de SegInfo nos órgãos e entidades da APF), das Normas Complementares (NCs) 8 e 18/IN01/DSIC/GSIPR (diretrizes para gerenciamento de incidentes em redes computacionais e para atividades de ensino em SegInfo nos órgãos e entidades da APF, respectivamente) e das normas ABNT NBR ISO/IEC 27001:2006, 20000-2:2008, 27005:2008 e 27002:2013, além de itens da biblioteca de referência em infraestrutura de TI *Information Technology Infrastructure Library* (ITIL) v3. Esses critérios são trazidos em seções específicas no bojo do Capítulo 3 e podem ser conferidos, também, no Anexo IV, peça 855.

18.Após o encaminhamento dos ofícios de comunicação do acompanhamento, realizado pela Secretaria de Gestão de Processos (Seproc) via Sistema Conecta, as interações com as organizações auditadas se deram, essencialmente, no bojo da plataforma LimeSurvey. Em um primeiro momento,

foi utilizada a versão 2.55+161021 apenas para a captura dos dados de contato (nome, cargo, e-mail e telefone) dos respondentes indicados por cada organização. Esses dados, então, foram alimentados em uma versão mais segura (*Community Edition*, versão 5.1.10+210913), na qual foi efetivamente aplicado o questionário. Adicionalmente, foram esclarecidas dúvidas recebidas por *e-mail* ou por telefone.

19.Uma vez definidos, na fase de planejamento, os objetivos do acompanhamento e a forma como ele seria conduzido, foi elaborada a Matriz de Planejamento para nortear o trabalho [...], bem como o questionário a ser aplicado aos respondentes indicados pelas organizações participantes, abrangendo os cinco controles críticos de SegCiber que seriam avaliados neste primeiro ciclo (parágrafos 7.1-7.5; Anexo I, peça 855).

20.Cada um desses controles foi, então, subdividido em duas perguntas específicas para cada uma das respectivas medidas de segurança previstas no *framework* do CIS. A primeira pergunta procurou identificar o grau geral de adoção daquela medida de segurança ("Não adota"; "Há decisão formal ou plano aprovado para adotá-la"; "Adota em menor parte"; "Adota parcialmente"; "Adota em maior parte ou totalmente"; "Não se aplica"). A segunda, então, buscou detalhar as subpráticas efetivamente implementadas na organização, relacionadas àquela medida de segurança. Por fim, todas essas perguntas foram encadeadas para formar o questionário *online* disponibilizado aos gestores.

21.Tendo em vista a existência de vinte medidas de segurança neste primeiro ciclo (Tabela 2, peça 855**Error! Reference source not found.**), o questionário ficou, então, com quarenta perguntas (duas para cada medida), mais uma pergunta final aberta, na última tela, que solicitava o registro, pelo respondente, dos principais desafios, deficiências e pontos de atenção relacionados à implantação desses controles e medidas de segurança, bem como outras considerações, comentários ou críticas que ele considerasse pertinentes.

22.O Capítulo 2 deste relatório reflete a forma com que o questionário foi estruturado, passando por cinco seções de perguntas específicas, cada uma relacionada a um dos cinco controles avaliados (Seções 2.1 a 2.5), além de outra relativa às respostas abertas fornecidas pelos gestores na última pergunta (Seção 2.6). Assim, o panorama geral das organizações públicas federais auditadas é apresentado ao longo das diferentes seções desse capítulo.

23.O Capítulo 3, então, apresenta os principais registros do primeiro ciclo do acompanhamento, isto é, os pontos que mais chamaram atenção dentre os controles e medidas de segurança avaliados nesta etapa da fiscalização, enquanto o Capítulo 4 descreve o painel (*dashboard*) que foi construído 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 os Capítulos 2 e 3, por exemplo, foram obtidas a partir desse painel.

24.A seu turno, o Capítulo 5 explica os propósitos deste acompanhamento e comenta sobre o relatório de *feedback* automatizado fornecido aos gestores respondentes ao final do preenchimento do questionário, de modo a ajudá-los a melhorar os controles avaliados, bem como sobre os relatórios comparativos de *feedback*, que ilustram o cenário de implementação desses controles em conjuntos de organizações com certa similaridade. Esse capítulo também descreve os indicadores criados no âmbito deste ciclo com a intenção de fornecer às organizações participantes medidas quantitativas relativas ao seu grau de maturidade geral em SegCiber (iSegCiber) e relacionadas especificamente a cada um dos cinco controles questionados (iControle1, iControle2, iControle7, iControle14 e iControle17).

25.O Capítulo 6 contextualiza o cenário atual de SegCiber no Brasil e no mundo, de modo a fornecer informações úteis aos gestores dos órgãos e entidades participantes deste acompanhamento, bem como ao Relator e aos demais ministros da Corte. O Capítulo 7, então, traz uma perspectiva para o futuro e sugere a "Estratégia de Fiscalização do TCU em SegInfo e Privacidade de Dados 2022-2025", atualização do documento que estabelece a estratégia de fiscalização do Tribunal nessas áreas.

26.Por fim, o Capítulo 8 apresenta a conclusão deste ciclo do acompanhamento, enquanto o Capítulo 9 contém as propostas de encaminhamento sugeridas em função da realização deste trabalho.

## 1.6. Limitações ocorridas

27.Uma possível limitação em fiscalizações que utilizam o método CSA diz respeito à qualidade das informações recebidas, tendo em vista o fato de o questionário (Anexo I, peça 855) ser, essencialmente, declarativo. Contudo, tendo em vista o caráter prioritariamente didático deste acompanhamento, esse não é um fator que gere preocupação. Cabe ao gestor respondente ter a maturidade de perceber que, numa resposta eventualmente superavaliada, a única pessoa que ele "enganou" foi a si mesmo.

28.Em todo caso, para minimizar esse efeito, no quarto e no sétimo ciclos do acompanhamento (Tabela 2, peça 855), os participantes deverão ser instados a anexar evidências que suportem as principais respostas fornecidas, com vistas a melhorar sua confiabilidade. A sistemática de execução desses ciclos "especiais", que envolverão a análise de evidências com vistas a identificar possíveis incongruências nas respostas, atendendo solicitação feita pelo Relator (peça 7), será elaborada oportunamente.

29.Adicionalmente, a depender do cenário diagnosticado ao final da execução de cada um dos ciclos deste acompanhamento, a equipe poderá propor a realização de auditorias apartadas envolvendo determinados controles de SegCiber e/ou organizações/setores específicos. Frise-se que, caso qualquer dessas fiscalizações venha a detectar ter ocorrido o envio, ao Tribunal, de informações que não correspondem à realidade da organização, o respectivo gestor respondente poderá ser penalizado com base na Lei 8.443/1992, art. 58, inciso VI, bem como no Regimento Interno do TCU, art. 268, inciso VI.

## 1.7. Visão geral do objeto

30. Este acompanhamento foi realizado para mapear a maturidade das organizações públicas federais quanto à implementação de controles críticos de SegCiber, de modo a dotar o TCU de inteligência suficiente para atuar proativamente no sentido de ajudar a aumentar a resiliência da APF frente a incidentes e ataques cibernéticos cada vez mais frequentes, contribuindo para o sucesso do processo de transformação digital do País. Assim, a fiscalização também teve a intenção de conscientizar e orientar os gestores de SegInfo em relação aos riscos decorrentes da ausência de controles de SegCiber e à necessidade urgente de implementá-los.

31.Com esses objetivos, tomou-se por base uma livre adaptação, a partir do julgamento profissional dos auditores, dos controles 1, 2, 7, 14 e 17 **Error! Reference source not found.**(Tabela 1, peça 855), bem como das respectivas medidas de segurança, constituintes da versão 8 do *framework* desenvolvido pelo CIS. A Tabela 1 enumera as vinte medidas de segurança específicas verificadas neste ciclo do acompanhamento. Cada uma delas é composta de diversas subpráticas, as quais foram detalhadas no questionário aplicado aos gestores.

**Tabela 1 - Controles 1, 2, 7, 14 e 17 do *framework* do CIS e respectivas medidas de segurança básicas (IG1).** (Fonte: *CIS Controls® Version* 8 [tradução livre])

| Controle | Medida de Segurança |
|---|---|
| **1) Inventário e controle de ativos corporativos** | |
| | 1.1 Estabelecer e manter um inventário detalhado de ativos corporativos |
| | 1.2 Tratar ativos não autorizados |
| **2) Inventário e controle de ativos de software** | |
| | 2.1 Estabelecer e manter um inventário de software |
| | 2.2 Assegurar que o software autorizado seja atualmente suportado |
| | 2.3 Tratar softwares não autorizados |
| **7) Gestão contínua de vulnerabilidades** | |
| | 7.1 Estabelecer e manter um processo de gestão de vulnerabilidades |
| | 7.2 Estabelecer e manter um processo de correção de vulnerabilidades |
| | 7.3 Executar a gestão automatizada de correções (*patches*) de sistemas operacionais |

| | |
|---|---|
| | 7.4 Executar a gestão automatizada de correções (*patches*) de aplicativos |
| **14) Conscientização sobre segurança e treinamento de competências** | |
| | 14.1 Estabelecer e manter um programa de conscientização em segurança |
| | 14.2 Treinar os colaboradores para reconhecerem ataques de engenharia social |
| | 14.3 Treinar os colaboradores em melhores práticas de autenticação de usuários |
| | 14.4 Treinar os colaboradores em melhores práticas de tratamento de dados |
| | 14.5 Treinar os colaboradores para evitarem exposição não intencional de dados |
| | 14.6 Treinar os colaboradores para reconhecerem e notificarem incidentes de segurança |
| | 14.7 Treinar os colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos |
| | 14.8 Treinar os colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras |
| **17) Gestão de respostas a incidentes** | |
| | 17.1 Designar responsáveis por gerenciar o tratamento de incidentes |
| | 17.2 Estabelecer e manter informações de contato para reporte de incidentes de segurança |
| | 17.3 Estabelecer e manter um processo para o recebimento de notificações de incidentes |

32. A metodologia utilizada no acompanhamento foi a autoavaliação de controles internos (CSA), tendo sido disponibilizado questionário, o qual foi respondido pelos gestores de modo a refletir os controles e medidas de segurança efetivamente implementados nas suas respectivas organizações (Seção 1.5 - Métodos utilizados).

## 2. Estruturação do acompanhamento

33. O acompanhamento foi estruturado na forma de questionário *online*, disponibilizado para preenchimento pelos gestores das organizações participantes e composto de uma sequência de telas, cada uma contendo perguntas relacionadas aos controles e medidas de segurança verificados, adaptadas pelos auditores com base na versão 8 do *framework* do CIS (Anexo I, peça 855), com vistas a fornecer o diagnóstico definido na Matriz de Planejamento.

34. As Seções 2.1 a 2.5 deste capítulo trazem os resultados gerais das organizações em relação às perguntas feitas acerca de cada um dos cinco controles questionados (1, 2, 7, 14 e 17) e suas respectivas medidas de segurança, bem como, quando pertinente, alguns comentários a respeito. Por fim, a Seção 2.6 procura condensar as manifestações feitas pelos gestores sobre os principais desafios, deficiências e pontos de atenção relacionados à implantação desses controles e medidas de segurança.

35. Ao final, as respostas fornecidas por todas as organizações participantes, tomadas em conjunto, serviram para a elaboração do Capítulo 3, bem como foram sintetizadas no Anexo IV, peça 855**Error! Reference source not found.**. Convém ressalvar, por oportuno, que esses "registros" são baseados, exclusivamente, nas respostas fornecidas pelos gestores ao questionário da fiscalização, não tendo sido, no presente ciclo, corroborados pela solicitação de evidências por parte dos auditores, procedimento previsto para ocorrer somente no quarto e no sétimo ciclos do acompanhamento (parágrafos 27-28).

### 2.1 Controle 1: Inventário e controle de ativos corporativos

36. Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todos os ativos corporativos de TI (*e.g.* equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos IoT; e servidores) conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (*cloud*

*computing*), com o objetivo de conhecer com precisão todos os ativos de hardware da organização que precisam ser monitorados e protegidos. Esse gerenciamento também ajuda a identificar equipamentos não autorizados e/ou não gerenciados, os quais devem ser removidos ou corrigidos.

37.Este controle é importante porque, dito de maneira simples, uma organização simplesmente não é capaz de defender aquilo que sequer sabe que possui. Nesse sentido, o controle dos ativos corporativos de TI desempenha papel crítico, por exemplo, na gestão de vulnerabilidades, no monitoramento de segurança, na resposta a incidentes, na execução de rotinas de *backup* e no processo de recuperação de incidentes. Uma organização também deve saber quais dados são essenciais ao seu negócio e, consequentemente, identificar os ativos corporativos que mantêm ou gerenciam tais dados, de modo a aplicar-lhes controles de segurança adequados.

38.Neste ciclo do acompanhamento, foram avaliadas duas medidas de segurança básicas (IG1) relacionadas a este controle (Tabela 1): 1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos; e 1.2 - Tratar ativos não autorizados.

Medida de segurança 1.1 - Estabelecer e manter um inventário detalhado de ativos corporativos

39. A Figura 1 traz as respostas das 377 organizações participantes à pergunta 1.1.1 do questionário: "A organização estabelece e mantém um inventário detalhado de ativos corporativos (inventário com informações precisas, detalhadas e atualizadas sobre todos os ativos de hardware da organização que, potencialmente, armazenam, transmitem e/ou processam dados)?". Verifica-se que a grande maioria das organizações (332) declararam que adotam essa prática, em alguma medida (em menor parte: 86; parcialmente: 110; em maior parte ou totalmente: 136), situação que era esperada, tendo em vista se tratar da medida de segurança mais básica do primeiro controle.

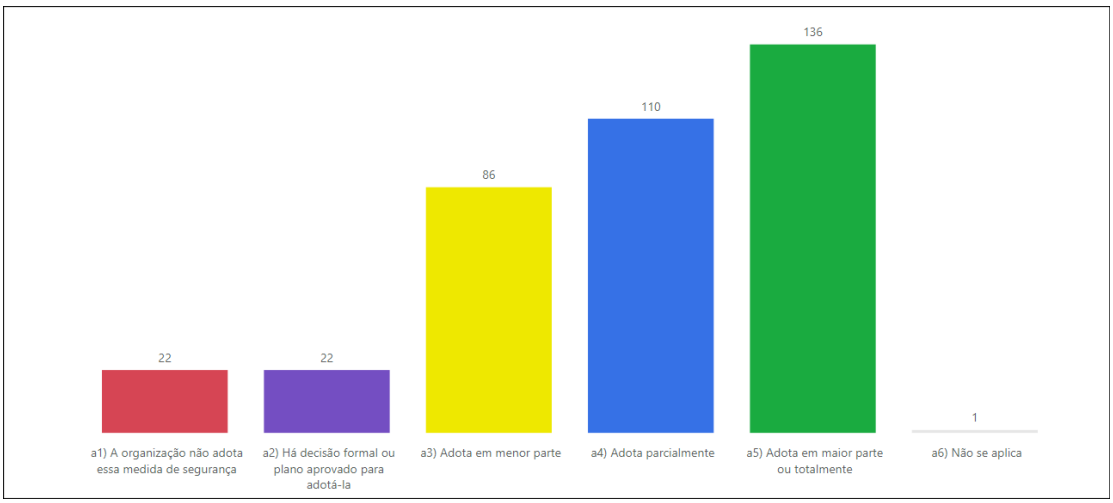



**Figura 1 - Distribuição das respostas à pergunta 1.1.1 do questionário.**
(1.1.1. A organização estabelece e mantém um inventário detalhado de ativos corporativos?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

40.Desconsideradas as 45 organizações que manifestaram não implementar tal medida (não adota: 22; há apenas decisão formal/plano para adotar: 22; não se aplica: 1), essas 332 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 1.1.2):

**Tabela 2 - Subpráticas da medida de segurança 1.1.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O inventário de ativos inclui dados dos equipamentos de usuários finais (incluindo computadores portáteis e dispositivos móveis)? | 225 | 107 |

| | | |
|---|---|---|
| O inventário de ativos inclui dados dos equipamentos servidores e dos dispositivos de rede? | 307 | 25 |
| O inventário de ativos inclui dados de dispositivos da Internet das Coisas (IoT)? | 29 | 303 |
| O inventário inclui, para cada ativo, informações básicas (*e.g.* nome, endereços de rede [se estático] e de hardware [MAC *address*], proprietário/responsável, local [dept., endereço]) e indicação se aquele ativo tem permissão/aprovação ou não para se conectar à rede? | 172 | 160 |
| A organização utiliza uma ferramenta de *Mobile Device Management* (MDM) para auxiliá-la a gerenciar os dispositivos móveis dos usuários finais? | 29 | 303 |
| O inventário inclui ativos conectados à infraestrutura da organização fisicamente, virtualmente e mesmo remotamente, incluindo aqueles em ambientes de nuvem (*cloud*)? | 141 | 191 |
| O inventário inclui ativos conectados regularmente à infraestrutura de rede da organização, mesmo que não estejam sob seu controle? | 86 | 246 |
| As informações constantes no inventário de ativos são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)? | 148 | 184 |

Medida de segurança 1.2 - Tratar ativos não autorizados

41.A Figura 2, a seu turno, mostra as respostas das 377 organizações à pergunta 1.2.1 do questionário: "A organização trata ativos não autorizados?". Percebe-se que grande contingente das organizações (210) manifestou que não implementa essa medida de segurança (não adota: 142; há apenas decisão formal/plano para adotar: 59; não se aplica: 9), o que é preocupante (Capítulo 3, Registro 1).

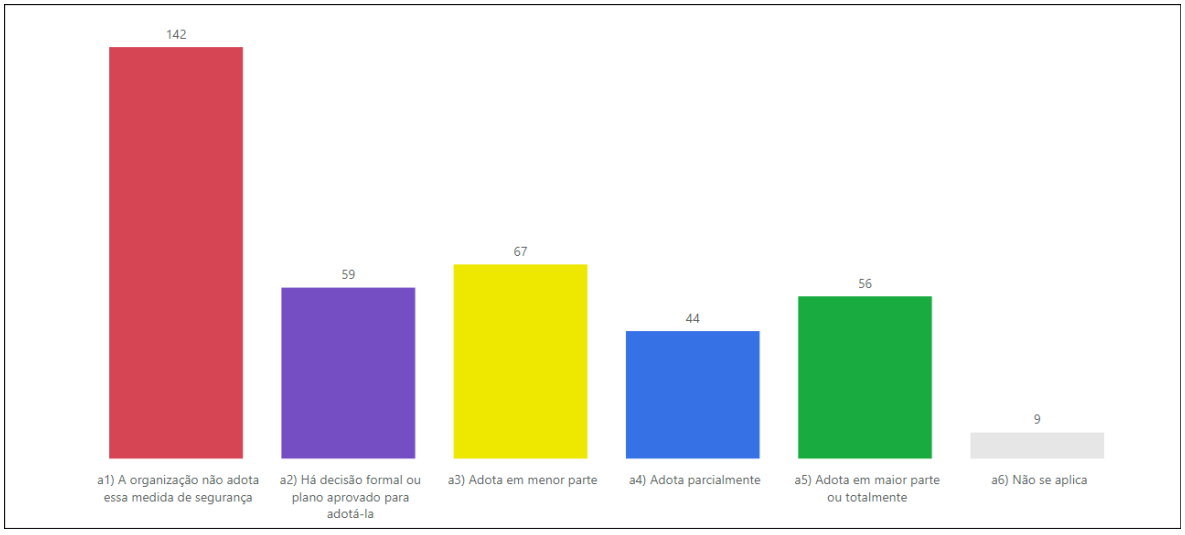



**Figura 2 - Distribuição das respostas à pergunta 1.2.1 do questionário.**
(1.2.1. A organização trata ativos não autorizados?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

42.Desconsideradas essas 210 organizações, as 167 restantes apresentaram o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 1.2.2):

**Tabela 3 - Subpráticas da medida de segurança 1.2.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O processo de tratamento dos ativos de hardware não autorizados ocorre semanalmente (ou ainda mais frequentemente)? | 43 | 124 |
| Quando detectado um ativo de hardware não autorizado, este é removido da rede da organização? | 139 | 28 |
| Quando detectado um ativo de hardware não autorizado, além de removido, a ele são negadas futuras tentativas de conexão à rede da organização? | 53 | 114 |
| Quando detectado um ativo de hardware não autorizado, este é colocado em "quarentena" (ambiente especialmente configurado para evitar que possa causar qualquer dano)? | 28 | 139 |

2.2 Controle 2: Inventário e controle de ativos de software

43. Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todo software (*e.g.* sistemas operacionais e aplicativos) utilizado de modo que somente softwares autorizados possam ser instalados e executados nas máquinas, ao mesmo tempo em que quaisquer softwares não autorizados e/ou não gerenciados sejam detectados e tenham sua instalação/execução impedida.

44. Possuir um inventário de software completo é fundamental para a prevenção de ataques, os quais, muitas vezes, têm início a partir de varreduras de rede que buscam encontrar versões vulneráveis de softwares que podem ser exploradas remotamente pelo atacante.

45. Por exemplo, um sistema ou aplicativo disponível na Internet por meio de uma versão vulnerável de servidor *web* pode ser derrubado remotamente e ficar indisponível (o que caracterizaria um ataque de negação de serviço [*Denial of Service* – DoS]), pode ser invadido e ter seu conteúdo adulterado (o que caracterizaria um ataque de pichação virtual [*defacement*]) ou, então, pode ter seus dados indevidamente capturados e expostos (o que caracterizaria um incidente de vazamento de dados). Outro exemplo de exploração remota acontece se um usuário recebe e abre um *e-mail* que o induz a clicar em um *link* para um sítio malicioso cujo conteúdo é carregado por uma versão vulnerável do navegador *web*, o que pode permitir que o atacante instale, no computador da vítima, algum programa que possibilite o seu controle remoto (o que caracterizaria um ataque de *phishing*).

46. Contra esses tipos de ataque, uma das principais defesas é manter todos os softwares sempre atualizados (ou seja, em versões nas quais as vulnerabilidades conhecidas já foram corrigidas) e, nesse sentido, um inventário completo ajuda a detectar se há algum software vulnerável e/ou desatualizado sendo utilizado ou, ainda, se há algum software não autorizado.

47. Neste ciclo do acompanhamento, foram avaliadas três medidas de segurança básicas (IG1) relacionadas a este controle (Tabela 1): 2.1 - Estabelecer e manter um inventário de software; 2.2 - Assegurar que o software autorizado seja atualmente suportado; e 2.3 - Tratar softwares não autorizados.

Medida de segurança 2.1 - Estabelecer e manter um inventário de software

48. A Figura 3 traz as respostas das 377 organizações participantes à pergunta 2.1.1 do questionário: "A organização estabelece e mantém um inventário detalhado de software (inventário com informações precisas, detalhadas e atualizadas sobre todos os softwares instalados nos ativos da organização, necessários para a realização das tarefas e rotinas corporativas diárias)?". Percebe-se que muitas organizações (108) manifestaram não implementar tal medida de segurança (não adota: 66; há apenas decisão formal/plano para adotar: 41; não se aplica: 1), o que é preocupante.

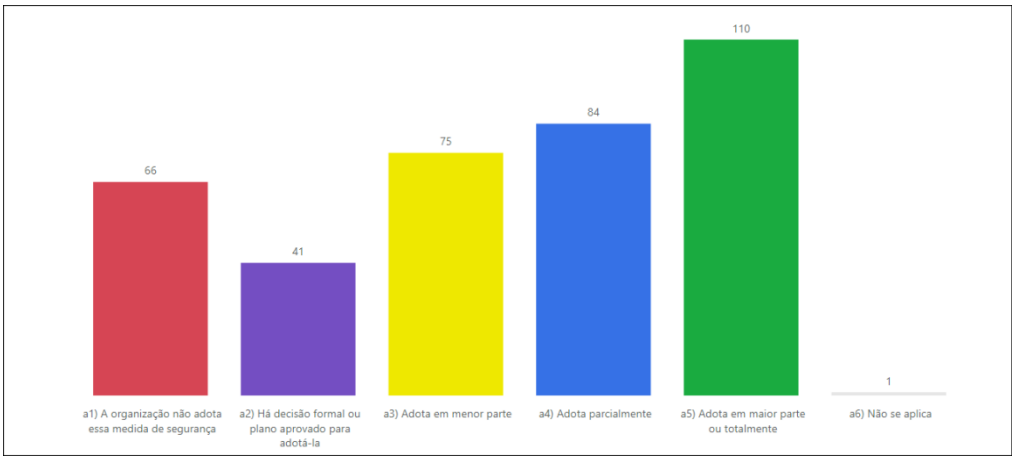



**Figura 3 - Distribuição das respostas à pergunta 2.1.1 do questionário.**
(2.1.1. A organização estabelece e mantém um inventário detalhado de software?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

49.Desconsideradas essas 108 organizações, as 269 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 2.1.2):

**Tabela 4 - Subpráticas da medida de segurança 2.1.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O inventário inclui informações básicas (*e.g.* título do software, empresa responsável [editor/*publisher*], data da instalação, respectivo propósito de negócio)? | 251 | 18 |
| Além das informações básicas, o inventário inclui informações adicionais sobre o software, tais como a URL de onde pode ser baixado, a indicação da(s) loja(s) de aplicativos, a versão, o respectivo mecanismo de implantação (*deployment*), a data de desativação etc.)? | 59 | 210 |
| As informações constantes no inventário de software são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)? | 109 | 160 |

Medida de segurança 2.2 - Assegurar que o software autorizado seja atualmente suportado

50.A Figura 4 apresenta as respostas das 377 organizações à pergunta 2.2.1 do questionário: "A organização assegura que apenas software atualmente suportado (previamente testado e homologado pelo setor de TI) seja designado como autorizado no inventário de software?". Percebe-se que um número considerável de organizações (112) declarou que não adota essa medida de segurança (não adota: 81; há apenas decisão formal/plano para adotar: 29; não se aplica: 2), o que é preocupante.

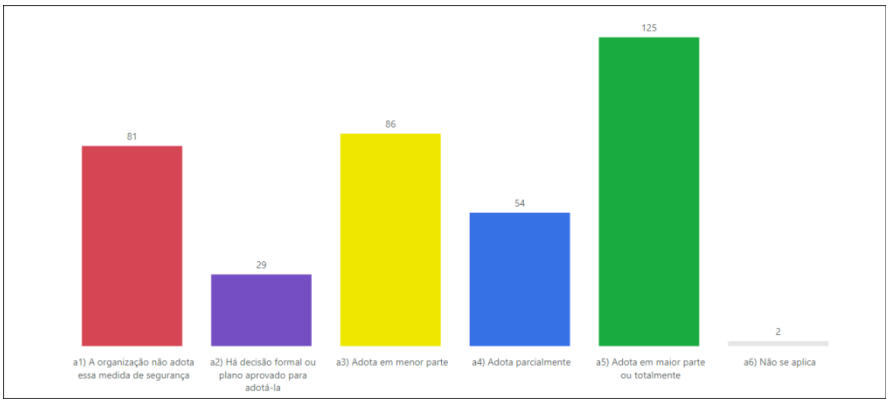



**Figura 4 - Distribuição das respostas à pergunta 2.2.1 do questionário.**
(2.2.1. A organização assegura que apenas software atualmente suportado seja designado como autorizado no inventário de software?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

51. Desconsideradas essas 112 organizações, as 265 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 2.2.2):

**Tabela 5 - Subpráticas da medida de segurança 2.2.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| Usuários "comuns" são impossibilitados de instalar qualquer software não autorizado nas máquinas da organização? | 255 | 10 |
| Todo software autorizado (e, portanto, suportado) é testado e homologado previamente pelo setor de TI da organização? | 195 | 70 |
| Caso, para atender aos objetivos do negócio da organização, seja necessário instalar/executar algum software ainda não suportado, é documentada uma exceção justificando a necessidade, detalhando os controles mitigatórios eventualmente adotados e declarando a aceitação dos riscos residuais? | 82 | 183 |
| Todo e qualquer software não suportado para o qual não tenha sido documentada uma exceção é designado como "não autorizado"? | 83 | 182 |
| O inventário de software é revisado mensalmente (ou ainda mais frequentemente) para detectar softwares não suportados? | 49 | 216 |

Medida de segurança 2.3 - Tratar softwares não autorizados

52. A Figura 5, a seu turno, mostra as respostas das 377 organizações à pergunta 2.3.1 do questionário: "A organização trata softwares não autorizados (softwares não suportados para os quais não tenha sido documentada uma exceção)?". Nota-se que muitas organizações (169) manifestaram que não implementam tal medida de segurança (não adota: 118; há apenas decisão formal/plano para adotar: 41; não se aplica: 10), o que caracteriza uma fragilidade (Capítulo 3, Registro 2).

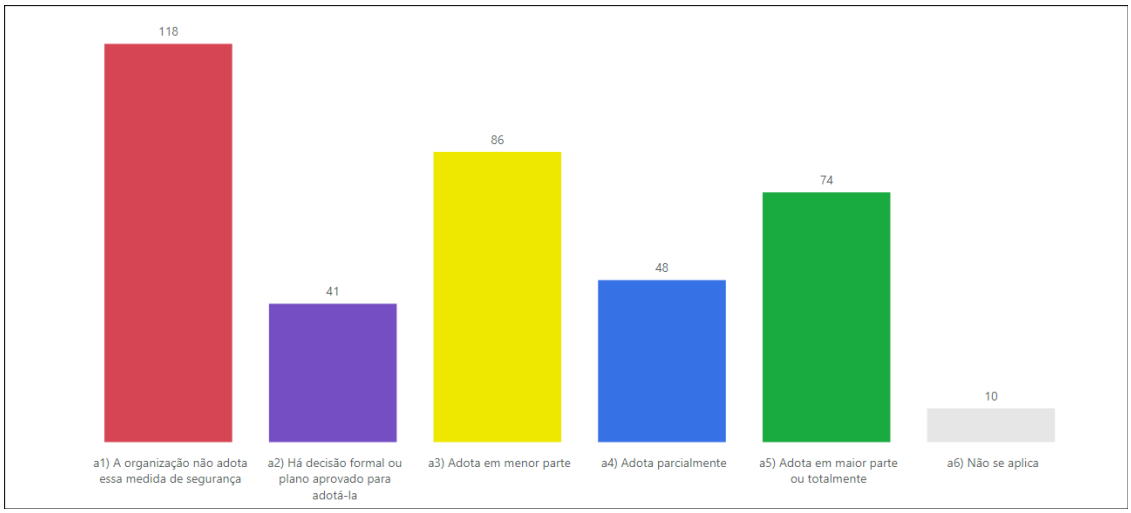



**Figura 5 - Distribuição das respostas à pergunta 2.3.1 do questionário.**
(2.3.1. A organização trata softwares não autorizados?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

53.Desconsideradas essas 169 organizações, as 208 restantes apresentaram o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 2.3.2):

**Tabela 6 - Subpráticas da medida de segurança 2.3.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O processo de tratamento dos softwares não autorizados ocorre mensalmente (ou ainda mais frequentemente)? | 42 | 166 |
| Quando detectado um software não autorizado, pode ser documentada uma exceção para autorizar seu uso, se necessário? | 133 | 75 |
| Quando detectado um software não autorizado e que não justifique a documentação de uma exceção, este é removido (desinstalado) do ativo? | 166 | 42 |

## 2.3 Controle 7: Gestão contínua de vulnerabilidades

54.Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

55.Este controle é crítico na medida em que se compreende que atacantes e defensores cibernéticos vivenciam uma disputa permanente, com os últimos sendo desafiados pelos primeiros, que procuram, constantemente, por vulnerabilidades que possam ser exploradas com sucesso. Nesse cenário, os defensores devem ter acesso tempestivo às informações disponíveis sobre as ameaças correntes e as respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes das suas organizações para identificar eventuais vulnerabilidades antes dos potenciais atacantes.

56.No entanto, como também têm acesso às mesmas informações que os defensores, os atacantes conseguem, frequentemente, aproveitar essas vulnerabilidades mais rapidamente do que as organizações conseguem corrigi-las. Daí a importância da gestão de vulnerabilidades, atividade contínua que requer tempo, atenção e recursos. Nos dias atuais, uma organização que não avalia

continuamente suas infraestruturas e softwares à procura de vulnerabilidades e proativamente corrige as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

57.Neste ciclo do acompanhamento, foram avaliadas quatro medidas de segurança básicas (IG1) relacionadas a este controle (Tabela 1): 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidades; 7.2 - Estabelecer e manter um processo de correção de vulnerabilidades; 7.3 - Executar a gestão automatizada de correções (*patches*) de sistemas operacionais; e 7.4 - Executar a gestão automatizada de correções (*patches*) de aplicativos.

Medida de segurança 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidades

58.A Figura 6 traz as respostas das 377 organizações participantes à pergunta 7.1.1 do questionário: "A organização estabelece e mantém um processo de gestão de vulnerabilidades (processo contínuo de avaliação e monitoramento dos ativos de hardware e software com vistas a eliminar, mitigar ou corrigir vulnerabilidades, bem como aprimorar configurações, controles e táticas de defesa)?". Nota-se que grande parte das organizações (215) manifestaram não implementar essa medida (não adota: 119; há apenas decisão formal/plano para adotar: 93; não se aplica: 3), infelizmente (Capítulo 3, Registro 3).

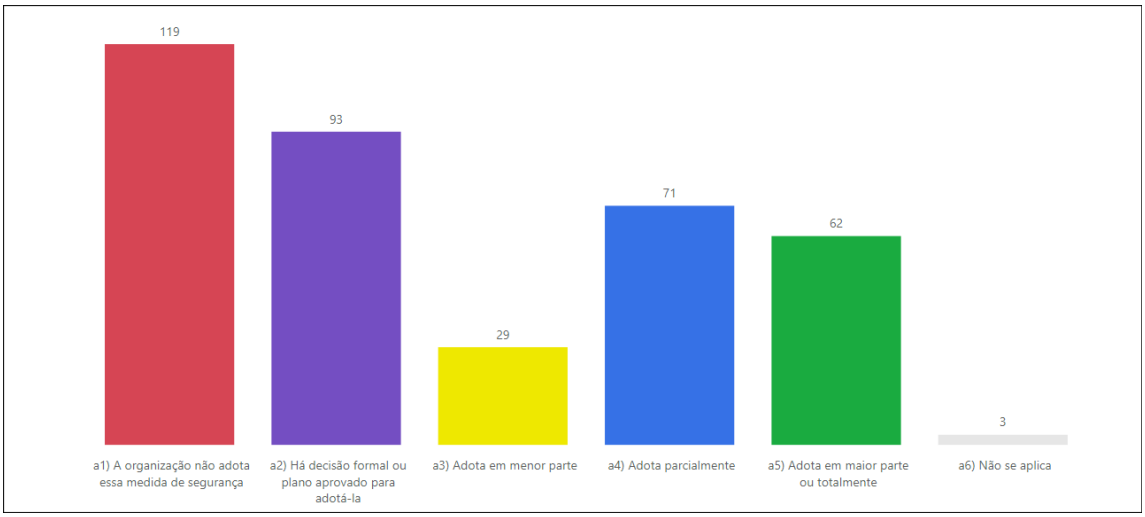



**Figura 6 - Distribuição das respostas à pergunta 7.1.1 do questionário.**
(7.1.1. A organização estabelece e mantém um processo de gestão de vulnerabilidades?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

59.Desconsideradas essas 215 organizações, as 162 restantes apresentaram o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 7.1.2):

**Tabela 7 - Subpráticas da medida de segurança 7.1.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O processo de gestão de vulnerabilidades está documentado? | 106 | 56 |
| O processo de gestão de vulnerabilidades está formalmente aprovado? | 60 | 102 |
| O processo de gestão de vulnerabilidades define os diversos papéis e responsabilidades associados, incluindo as atividades de monitoramento de vulnerabilidades, avaliação de risco de vulnerabilidades, aplicação de correções e acompanhamento dos ativos, bem como o desempenho da | 65 | 97 |

| | | |
|---|---|---|
| função de coordenação e a documentação associada a essas atividades? | | |
| O processo de gestão de vulnerabilidades é revisado e atualizado anualmente (ou ainda mais frequentemente)? | 41 | 121 |
| Independentemente da revisão periódica, o processo de gestão de vulnerabilidades é atualizado sempre que a organização passa por uma mudança significativa que pode impactá-lo? | 85 | 77 |

Medida de segurança 7.2 - Estabelecer e manter um processo de correção de vulnerabilidades

60.A Figura 7, a seu turno, traz as respostas das 377 organizações à pergunta 7.2.1 do questionário: "A organização estabelece e mantém um processo de correção de vulnerabilidades (processo de avaliação periódica das vulnerabilidades identificadas e dos riscos a elas associados, priorizando a aplicação de medidas mitigatórias de modo a aumentar a efetividade dos esforços de proteção)?". Percebe-se que muitas organizações (176) também manifestaram que não implementam tal medida de segurança (não adota: 103; há apenas decisão formal/plano para adotar: 71; não se aplica: 2), situação que demanda atenção (Capítulo 3, Registro 3).

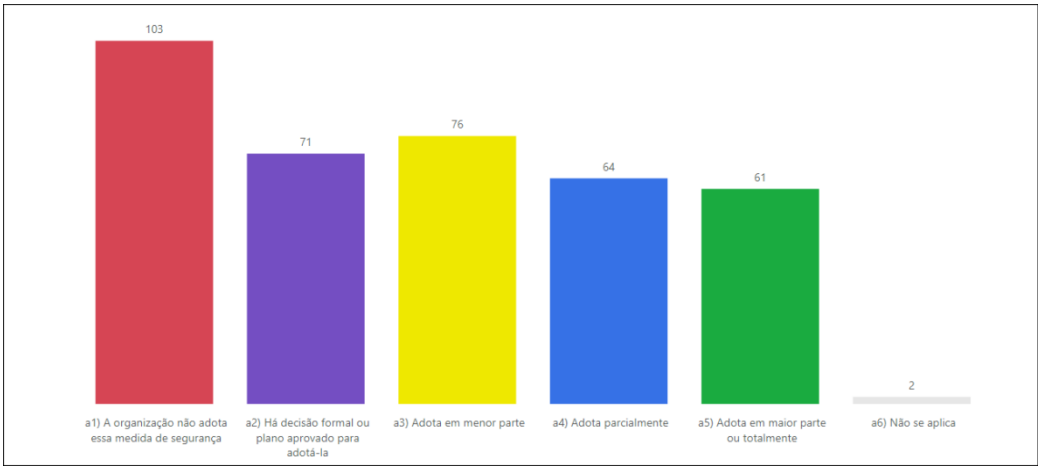



**Figura 7 - Distribuição das respostas à pergunta 7.2.1 do questionário.**
(7.2.1. A organização estabelece e mantém um processo de correção de vulnerabilidades?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

61.Desconsideradas essas 176 organizações, as 201 restantes apresentaram o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 7.2.2):

**Tabela 8 - Subpráticas da medida de segurança 7.2.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O processo de correção de vulnerabilidades está documentado? | 81 | 120 |
| O processo de correção de vulnerabilidades está formalmente aprovado? | 57 | 144 |
| As correções das vulnerabilidades identificadas são priorizadas de acordo com os respectivos riscos (derivados de avaliações de probabilidade | 167 | 34 |

| | | |
|---|---|---|
| e impacto no negócio, por exemplo, para cada vulnerabilidade)? | | |
| As vulnerabilidades e seus respectivos riscos são revisados mensalmente (ou ainda mais frequentemente)? | 68 | 133 |

Medida de segurança 7.3 - Executar a gestão automatizada de correções (*patches*) de sistemas operacionais

62.A Figura 8 traz as respostas das 377 organizações à pergunta 7.3.1 do questionário: "A organização executa a gestão automatizada da aplicação de correções/*patches* (programas criados para atualizar ou corrigir um software, sanando erros de comportamento, *bugs* ou vulnerabilidades de segurança e/ou melhorando sua usabilidade ou performance) nos sistemas operacionais dos seus ativos?". Nota-se que poucas organizações (86) manifestaram não implementar essa medida de segurança (não adota: 68; há apenas decisão formal/plano para adotar: 15; não se aplica: 3), situação que surpreendeu positivamente a equipe do acompanhamento (Capítulo 3, Registro 4).

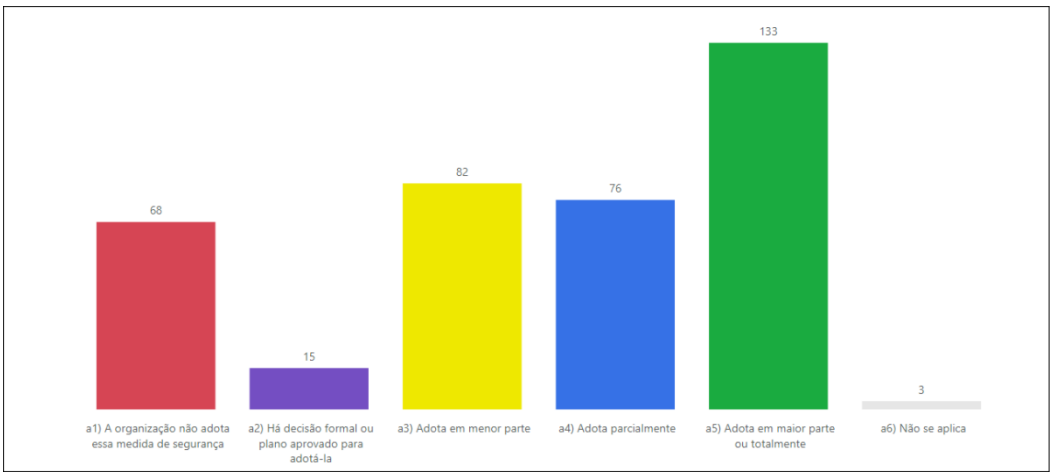



**Figura 8 - Distribuição das respostas à pergunta 7.3.1 do questionário.**
(7.3.1. A organização executa a gestão automatizada da aplicação de correções/*patches* nos sistemas operacionais dos seus ativos?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

63.Desconsideradas essas 86 organizações, as 291 restantes apresentaram o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 7.3.2):

**Tabela 9 - Subpráticas da medida de segurança 7.3.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas a seus sistemas operacionais, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados? | 207 | 84 |
| A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos? | 227 | 64 |

| | | |
|---|---|---|
| As correções (*patches*) de sistemas operacionais são testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão e que não tragam novos riscos e/ou causem efeitos adversos intoleráveis? | 147 | 144 |
| A verificação da necessidade de atualização/aplicação de correções (*patches*) nos sistemas operacionais ocorre mensalmente (ou ainda mais frequentemente)? | 171 | 120 |

Medida de segurança 7.4 - Executar a gestão automatizada de correções (*patches*) de aplicativos

64. A Figura 9, a seu turno, mostra as respostas das 377 organizações à pergunta 7.4.1 do questionário: "A organização executa a gestão automatizada da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos?". Ao contrário da medida anterior, percebe-se que muitas organizações (150) declararam que não adotam essa medida de segurança (não adota: 119; há apenas decisão formal/plano para adotar: 28; não se aplica: 3), o que é um tanto preocupante.

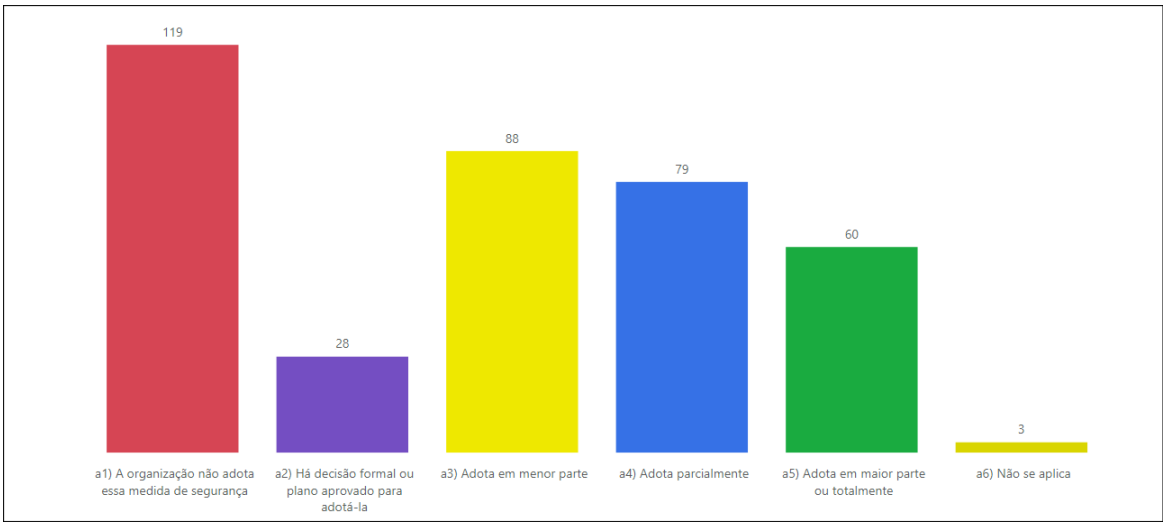



**Figura 9 - Distribuição das respostas à pergunta 7.4.1 do questionário.**
(7.4.1. A organização executa a gestão automatizada da aplicação de correções/*patches* nos aplicativos/programas dos seus ativos?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

65. Desconsideradas essas 150 organizações, as 227 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 7.4.2):

**Tabela 10 - Subpráticas da medida de segurança 7.4.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas a seus aplicativos/programas, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados? | 170 | 57 |

| | | |
|---|---|---|
| A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos? | 135 | 92 |
| As correções (*patches*) de aplicativos (programas) são testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão e que não tragam novos riscos e/ou causem efeitos adversos intoleráveis? | 112 | 115 |
| A verificação da necessidade de atualização/aplicação de correções (*patches*) nos aplicativos (programas) ocorre mensalmente (ou ainda mais frequentemente)? | 97 | 130 |

2.4 Controle 14: Conscientização sobre segurança e treinamento de competências

66. Visão geral: estabelecer e manter um programa contínuo e permanente de conscientização e treinamento para que os colaboradores tenham conhecimentos adequados em segurança (da informação e cibernética) e, consequentemente, adotem comportamentos e procedimentos seguros de modo a reduzir os riscos para a organização.

67. Este controle é essencial, tendo em vista que, quando se trata do tripé da segurança da informação, formado por tecnologia, processos e pessoas, essas últimas representam, provavelmente, o principal ponto de fragilidade (no jargão da área, são "o elo mais fraco da corrente"). A título de exemplo, é bem mais fácil um invasor ter sucesso buscando induzir um usuário a clicar em um *link* ou a abrir um anexo de e-mail (e, com isso, instalar um software malicioso no computador da vítima) do que tentando explorar e aproveitar diretamente alguma vulnerabilidade de rede.

68. Ademais, os colaboradores, intencionalmente ou não, podem causar incidentes de segurança por meio de diversas outras ações, tais como o envio de e-mail com dados sensíveis para o destinatário errado, a perda de um equipamento/dispositivo portátil (*e.g.* notebook, *pendrive*), a utilização de senhas fracas ou a reutilização da mesma senha usada para autenticação em um sítio público.

69. Assim, tem-se que os programas corporativos de segurança (da informação e cibernética), em grande medida, têm seu sucesso ou fracasso determinados por essa variável (nível de conscientização e treinamento dos colaboradores), sendo que nenhum desses programas consegue reduzir os riscos da organização a níveis aceitáveis sem considerar e endereçar a componente relativa ao comportamento humano, visto que, mesmo de formas não intencionais, os usuários podem causar incidentes de segurança.

70. Neste ciclo do acompanhamento, foram avaliadas oito medidas de segurança básicas (IG1) relacionadas a este controle (Tabela 1): 14.1 - Estabelecer e manter um programa de conscientização em segurança; 14.2 - Treinar os colaboradores para reconhecerem ataques de engenharia social; 14.3 - Treinar os colaboradores em melhores práticas de autenticação de usuários; 14.4 - Treinar os colaboradores em melhores práticas de tratamento de dados; 14.5 - Treinar os colaboradores para evitarem exposição não intencional de dados; 14.6 - Treinar os colaboradores para reconhecerem e notificarem incidentes de segurança; 14.7 - Treinar os colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos; e 14.8 - Treinar os colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras.

Medida de segurança 14.1 - Estabelecer e manter um programa de conscientização em segurança

71. A Figura 10 apresenta as respostas das 377 organizações à pergunta 14.1.1 do questionário: "A organização estabelece e mantém um programa de conscientização em segurança (programa contínuo e permanente de treinamento com vistas a mostrar aos colaboradores os riscos e ameaças aos quais os ativos e dados da organização estão sujeitos e como agir para evitá-los/mitigá-los)?". Percebe-se que a maioria das organizações (219) manifestaram que não implementam essa medida de segurança (não adota: 134; há apenas decisão formal/plano para adotar: 84; não se aplica: 1), o que é muito preocupante (Capítulo 3, Registro 5).

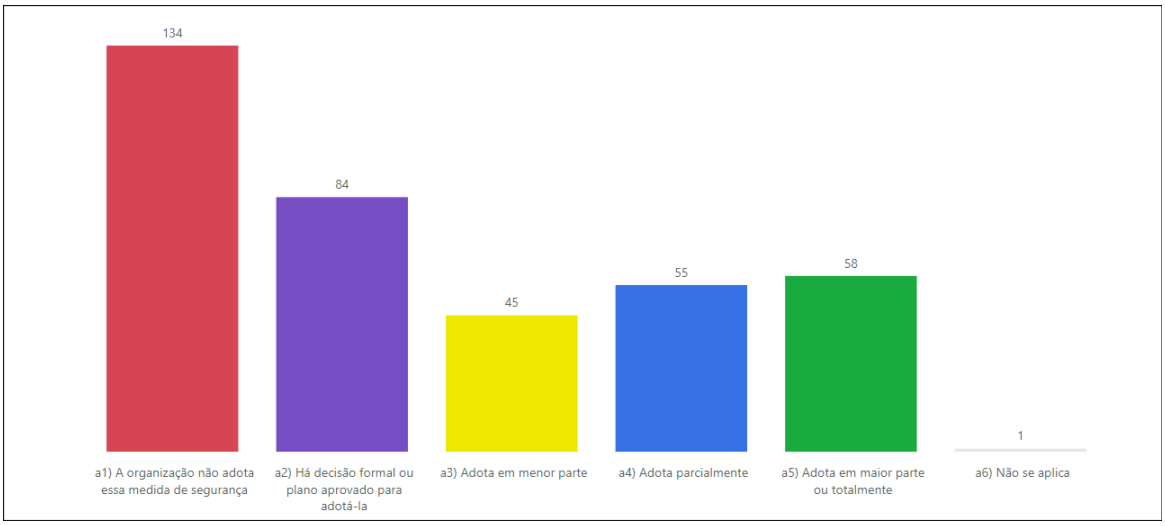



**Figura 10 - Distribuição das respostas à pergunta 14.1.1 do questionário.**
(14.1.1. A organização estabelece e mantém um programa de conscientização em segurança?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

72.Desconsideradas essas 219 organizações, as 158 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.1.2):

**Tabela 11 - Subpráticas da medida de segurança 14.1.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O programa de conscientização em segurança está documentado? | 81 | 77 |
| O programa de conscientização em segurança está formalmente aprovado? | 76 | 82 |
| Os colaboradores recebem treinamento geral em segurança (como lidar com os ativos/dados corporativos de maneira segura) logo após sua contratação? | 66 | 92 |
| Os colaboradores recebem treinamento geral em segurança anualmente (ou ainda mais frequentemente)? | 76 | 82 |
| O programa de conscientização em segurança considera os diferentes papéis desempenhados pelos colaboradores? | 66 | 92 |
| Antes de assumirem novas posições na organização, os colaboradores recebem treinamento específico para os requisitos de segurança dos papéis a serem desempenhados? | 20 | 138 |
| O conteúdo do programa de conscientização em segurança é revisado e atualizado anualmente (ou ainda mais frequentemente)? | 71 | 87 |
| Independentemente da revisão periódica, o conteúdo do programa de conscientização em segurança é atualizado sempre que a organização passa por uma mudança significativa que pode impactá-lo? | 67 | 91 |

Medida de segurança 14.2 - Treinar os colaboradores para reconhecerem ataques de engenharia social

73.A Figura 11, a seu turno, sintetiza as respostas das 377 organizações à pergunta 14.2.1 do questionário: "A organização treina seus colaboradores para reconhecerem ataques de engenharia social (manipulação psicológica de indivíduos para que executem ações que não deveriam ou, então, que divulguem informações confidenciais, sigilosas ou sensíveis)?". Nota-se que quase dois terços das organizações (239) declararam não adotar essa medida de segurança (não adota: 162; há apenas decisão formal/plano para adotar: 75; não se aplica: 2), situação que também preocupa (Capítulo 3, Registro 5).

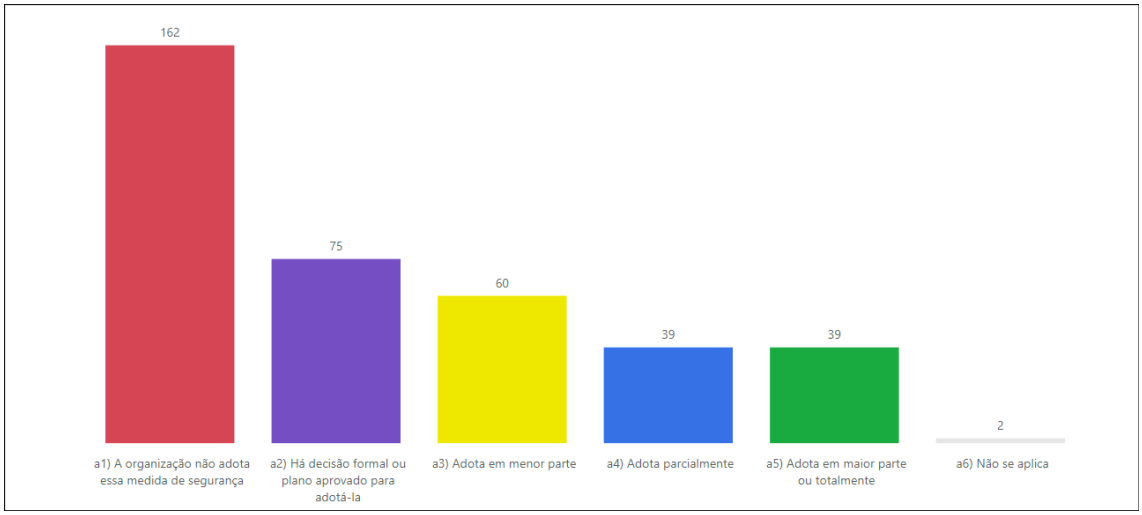



**Figura 11 - Distribuição das respostas à pergunta 14.2.1 do questionário.**
(14.2.1. A organização treina seus colaboradores para reconhecerem ataques de engenharia social?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

74.Desconsideradas essas 239 organizações, as 138 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.2.2):

**Tabela 12 - Subpráticas da medida de segurança 14.2.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda ataques do tipo *phishing*? | 137 | 1 |
| O treinamento aborda técnicas de pretexto (*pre-texting*)? | 55 | 83 |
| O treinamento aborda técnicas de "isca"? | 54 | 84 |
| O treinamento aborda ataques do tipo quiproquó (*quid pro quo*)? | 27 | 111 |
| O treinamento aborda ataques do tipo "carona" (*tailgating*)? | 29 | 109 |

*As explicações sobre cada um desses tipos de ataque podem ser encontradas no **Error! Reference source not found.** (pergunta 14.2.2).

Medida de segurança 14.3 - Treinar os colaboradores em melhores práticas de autenticação de usuários

75.A Figura 12 sintetiza as respostas das 377 organizações à pergunta 14.3.1 do questionário: "A organização treina seus colaboradores em melhores práticas de autenticação de usuários (mecanismo pelo qual é possível atestar que um usuário [de determinado sistema, por exemplo] é legítimo, ou

seja, que ele realmente é quem afirma ser)?". Percebe-se que mais da metade das organizações (202) declararam não implementar essa medida de segurança (não adota: 141; há apenas decisão formal/plano para adotar: 59; não se aplica: 2), o que é igualmente preocupante (Capítulo 3, Registro 5).

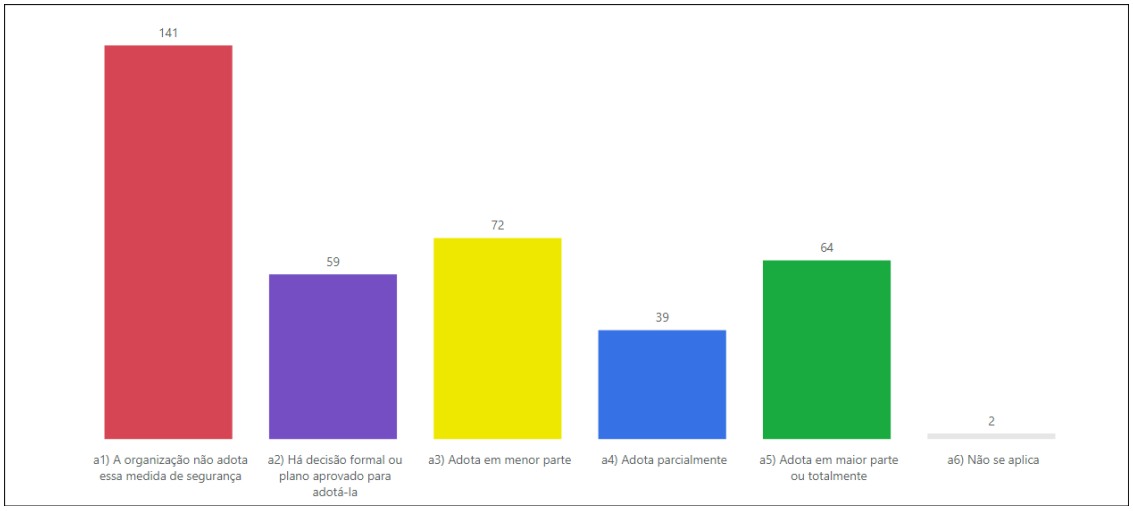



**Figura 12 - Distribuição das respostas à pergunta 14.3.1 do questionário.**
(14.3.1. A organização treina seus colaboradores em melhores práticas de autenticação de usuários?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

76.Desconsideradas essas 202 organizações, as 175 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.3.2):

**Tabela 13 - Subpráticas da medida de segurança 14.3.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda dicas para composição de senhas seguras/fortes? | 166 | 9 |
| O treinamento aborda aspectos relativos à guarda das senhas, incluindo ferramentas específicas de gerenciamento de credenciais? | 76 | 99 |
| O treinamento aborda autenticação multifator (*multi-factor authentication* – MFA)? | 93 | 82 |

*As explicações sobre senhas seguras/fortes, gerenciadores de senhas e fatores de autenticação podem ser encontradas no **Error! Reference source not found.** (pergunta 14.3.2).

Medida de segurança 14.4 - Treinar os colaboradores em melhores práticas de tratamento de dados

77.A Figura 13 sintetiza as respostas das 377 organizações à pergunta 14.4.1 do questionário: "A organização treina seus colaboradores em melhores práticas de tratamento de dados (identificar dados sensíveis no contexto da organização e, consequentemente, saber como armazená-los, transferi-los, arquivá-los e destruí-los adequadamente, de modo a minimizar os riscos de vazamento)?". Nota-se que mais de dois terços das organizações (259) declararam que não adotam essa medida de segurança (não adota: 164; há apenas decisão formal/plano para adotar: 93; não se aplica: 2), o que é muito preocupante (Capítulo 3, Registro 5).

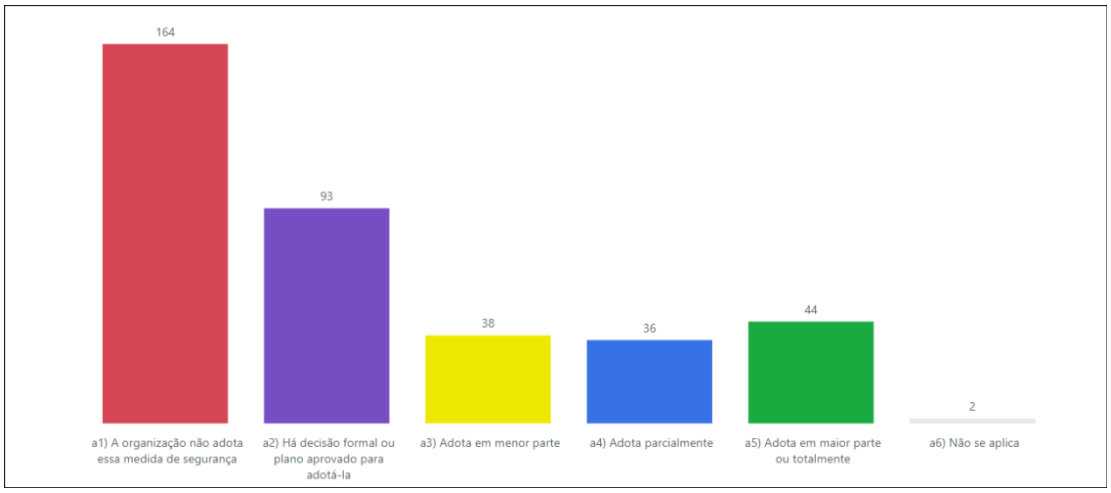



**Figura 13 - Distribuição das respostas à pergunta 14.4.1 do questionário.**
(14.4.1. A organização treina seus colaboradores em melhores práticas de tratamento de dados?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

78.Desconsideradas essas 259 organizações, as 118 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.4.2):

**Tabela 14 - Subpráticas da medida de segurança 14.4.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda a "política de mesa limpa e tela limpa"? | 85 | 33 |
| A organização possui uma política de classificação da informação formalmente aprovada, cujo conteúdo faz parte do escopo do treinamento? | 67 | 51 |
| O treinamento aborda a proteção das informações contidas em ativos portáteis (*e.g. notebooks*, *tablets*, celulares, mídias removíveis), a exemplo do armazenamento apenas dos arquivos estritamente essenciais e da aplicação de mecanismos de proteção criptográfica? | 67 | 51 |
| O treinamento aborda aspectos relacionados à deleção permanente de arquivos e dados (*data wiping*) e ao descarte seguro de mídias/equipamentos? | 36 | 82 |

*As explicações sobre a "política de mesa limpa e tela limpa" e a política de classificação da informação podem ser encontradas no Anexo I, peça 855 (pergunta 14.4.2).

Medida de segurança 14.5 - Treinar os colaboradores para evitarem exposição não intencional de dados

79.A Figura 14 sintetiza as respostas das 377 organizações à pergunta 14.5.1 do questionário: "A organização treina seus colaboradores para evitarem exposição não intencional de dados (*e.g.* perda/extravio de dispositivos portáteis, envio de informações sensíveis ao destinatário errado, publicação de dados para uma audiência que não deveria ter acesso a eles)?". Tem-se que a grande maioria das organizações (263) declarou não adotar essa medida de segurança (não adota: 181; há apenas decisão formal/plano para adotar: 80; não se aplica: 2), o que também preocupa (Capítulo 3, Registro 5).

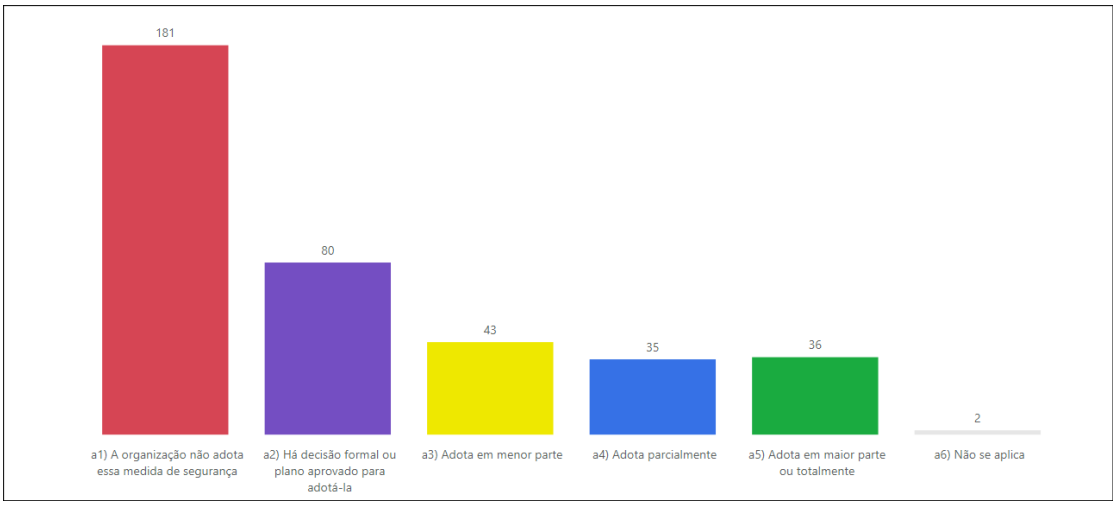



**Figura 14 - Distribuição das respostas à pergunta 14.5.1 do questionário.**
(14.5.1. A organização treina seus colaboradores para evitarem exposição não intencional de dados?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

80.Desconsideradas essas 263 organizações, as 114 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.5.2):

**Tabela 15 - Subpráticas da medida de segurança 14.5.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda a adoção de cuidados gerais quanto à guarda e ao uso de equipamentos portáteis (*e.g. notebooks*, *tablets*, celulares, mídias removíveis)? | 85 | 29 |
| O treinamento aborda a conferência dos destinatários antes do envio de comunicações (*e.g.* e-mails) que contenham informações sensíveis? | 68 | 46 |
| O treinamento aborda aspectos relacionados à publicação de conteúdos da organização em aplicativos de mensageria e/ou em redes sociais? | 79 | 35 |

Medida de segurança 14.6 - Treinar os colaboradores para reconhecerem e notificarem incidentes de segurança

81.A Figura 15 sintetiza as respostas das 377 organizações à pergunta 14.6.1 do questionário: "A organização treina seus colaboradores para reconhecerem e notificarem incidentes de segurança (eventos indesejados/inesperados que podem comprometer a operação do negócio e/ou colocar em risco a preservação da confidencialidade, integridade, disponibilidade ou autenticidade das informações)?". Percebe-se, novamente, que a grande maioria das organizações (263) manifestou não implementar essa medida de segurança (não adota: 175; há apenas decisão formal/plano para adotar: 86; não se aplica: 2), situação que, de igual modo, demanda atenção (Capítulo 3, Registro 5).

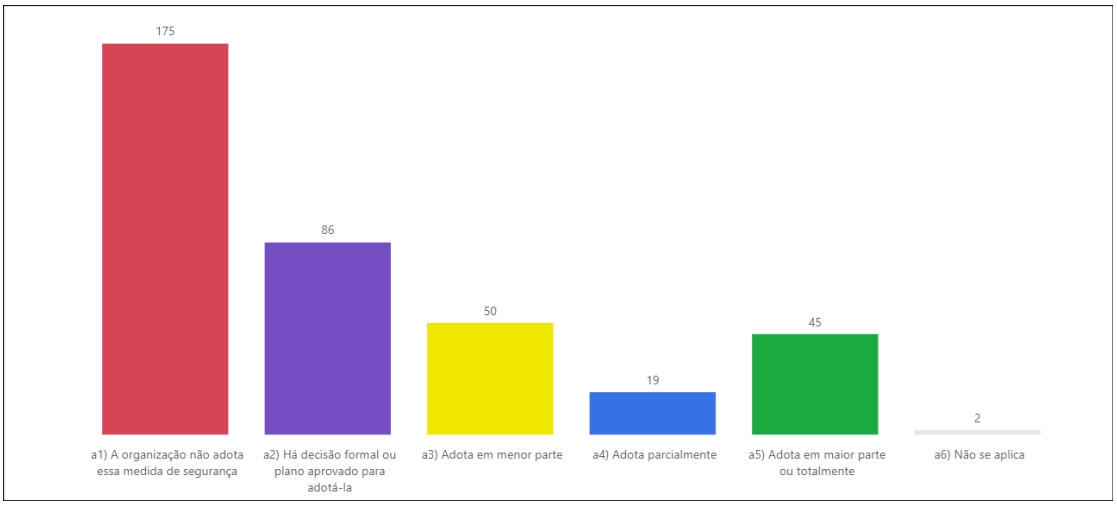



**Figura 15 - Distribuição das respostas à pergunta 14.6.1 do questionário.**
(14.6.1. A organização treina seus colaboradores para reconhecerem e notificarem incidentes de segurança?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

82.Desconsideradas essas 263 organizações, as 114 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.6.2):

**Tabela 16 - Subpráticas da medida de segurança 14.6.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda os principais vetores de ataque (*e.g.* mídias removíveis, sítios/e-mails maliciosos, perda/furto de equipamentos) e como cada um destes pode ser explorado? | 89 | 25 |
| O treinamento aborda os sinais precursores e indicadores da ocorrência de incidentes? | 37 | 77 |
| Além de ensinar os colaboradores a reconhecerem os sinais da ocorrência de incidentes, o treinamento os capacita a identificarem o tipo, a extensão e a magnitude do problema? | 41 | 73 |
| Além de capacitar os colaboradores a reconhecerem incidentes de segurança, o treinamento lhes ensina os canais e os meios apropriados para a respectiva notificação? | 85 | 29 |

*As explicações sobre sinais precursores e indicadores podem ser encontradas no **Error! Reference source not found.** (pergunta 14.6.2).

Medida de segurança 14.7 - Treinar os colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos

83.A Figura 16 sintetiza as respostas das 377 organizações à pergunta 14.7.1 do questionário: "A organização treina seus colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos (ativos com versões de software desatualizadas e/ou sem a instalação dos pacotes de correções mais recentes, bem como ativos em que a execução dos processos/ferramentas automatizados de aplicação dessas correções tenha apresentado alguma falha/erro)?". Nota-se que 83,6% das organizações (315) disseram não adotar essa medida de segurança (não adota: 251; há apenas decisão formal/plano para adotar: 52; não se aplica: 12), o que é muito preocupante (Capítulo 3, Registro 5).

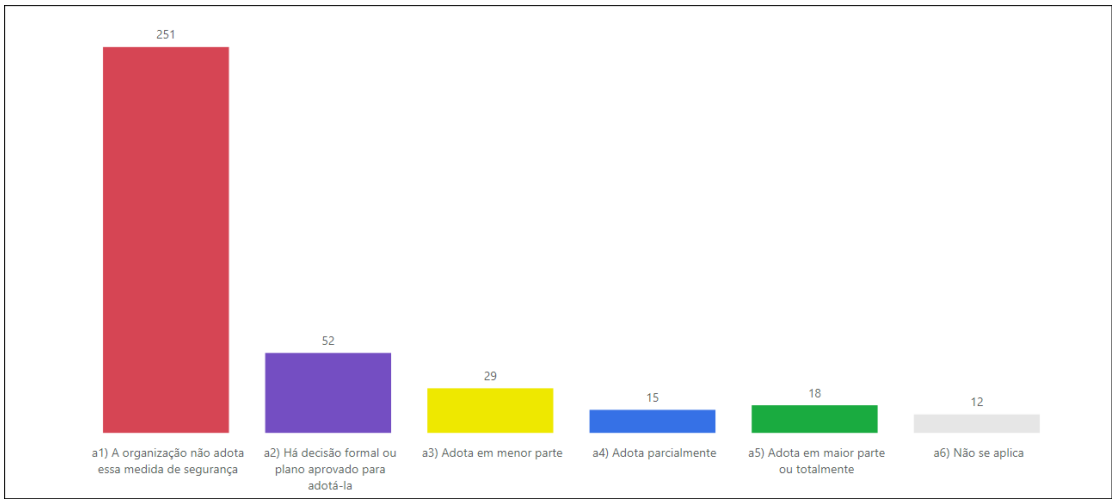



**Figura 16 - Distribuição das respostas à pergunta 14.7.1 do questionário.**
(14.7.1. A organização treina seus colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

84.Desconsideradas essas 315 organizações, as 62 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.7.2):

**Tabela 17 - Subpráticas da medida de segurança 14.7.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento capacita os colaboradores a verificarem se as versões dos softwares e dos pacotes de correções (*patches*) instalados nos ativos corporativos estão desatualizadas? | 33 | 29 |
| O treinamento ensina os colaboradores a reconhecerem a ocorrência de falhas na execução de processos/ferramentas automatizados (mensagens de erro, análise de *logs* etc.)? | 22 | 40 |
| O treinamento reforça a necessidade de notificação ao setor de TI sempre que identificada alguma das ocorrências descritas nos itens anteriores? | 43 | 19 |

Medida de segurança 14.8 - Treinar os colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras

85.A Figura 17 sintetiza as respostas das 377 organizações à pergunta 14.8.1 do questionário: "A organização treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras (que não implementam medidas básicas de segurança como a autenticação de usuários e a criptografia e, em geral, também não são protegidas por soluções antivírus ou *firewalls*)?". Percebe-se que três quartos das organizações (285) declararam que não adotam essa medida de segurança (não adota: 203; há apenas decisão formal/plano para adotar: 74; não se aplica: 8), situação que, também, preocupa bastante (Capítulo 3, Registro 5).

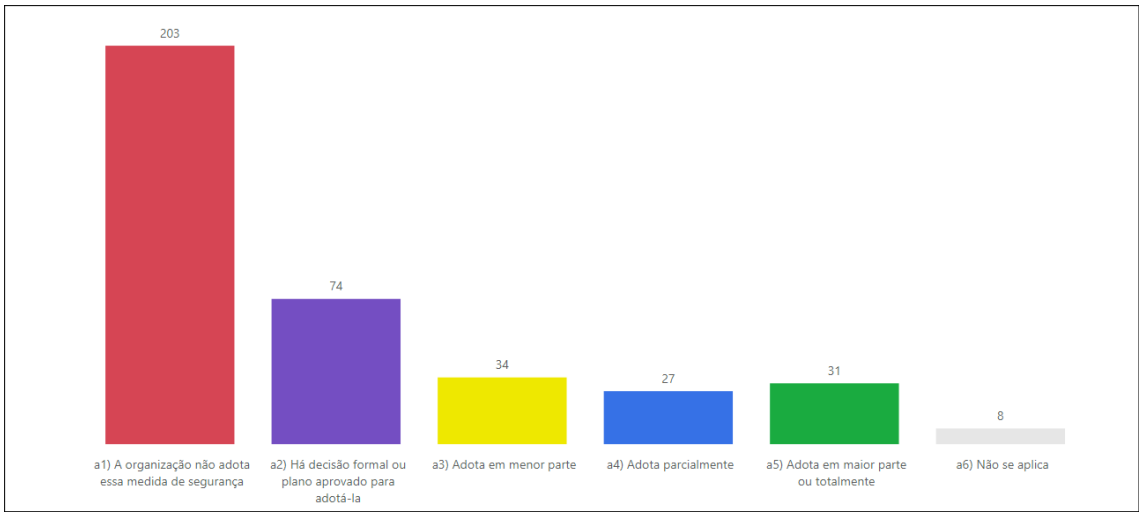



**Figura 17 - Distribuição das respostas à pergunta 14.8.1 do questionário.**
(14.8.1. A organização treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

86.Desconsideradas essas 285 organizações, as 92 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 14.8.2):

**Tabela 18 - Subpráticas da medida de segurança 14.8.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|
| O treinamento aborda os riscos envolvidos na conexão a redes inseguras (*e.g.* captura de credenciais/senhas, comprometimento do ativo a partir da instalação de um *malware*)? | 75 | 17 |
| O treinamento aborda os riscos envolvidos na transmissão de dados por meio de redes inseguras (*e.g.* vazamento ou adulteração dos dados, exposição de dados pessoais)? | 66 | 26 |
| O treinamento aborda a evolução histórica dos protocolos de criptografia de redes wi-fi (WEP, WPA e WPA2) e suas diferenças em termos da segurança das respectivas conexões? | 10 | 82 |
| O treinamento capacita os colaboradores que atuam em regime de trabalho remoto a configurarem sua infraestrutura de rede local de modo a aumentarem a segurança das conexões? | 54 | 38 |

*As explicações sobre os protocolos WEP, WPA e WPA2 podem ser encontradas no **Error! Reference source not found.** (pergunta 14.8.2).

## 1.8. Controle 17: Gestão de respostas a incidentes

87.Visão geral: estabelecer um programa para desenvolver e manter capacidade de resposta a incidentes de segurança da informação (*e.g.* políticas, planos, procedimentos, definição de papeis, treinamento e comunicação), de modo a estar preparado para detectar e responder rapidamente a ataques.

88.Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes acontecerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso ocorrer. Os principais objetivos da gestão de respostas a incidentes, então, são identificar potenciais ameaças, responder a elas antes que se espalhem, corrigi-las antes que causem danos e recuperar dados e sistemas eventualmente corrompidos.

89.Neste ciclo do acompanhamento, foram avaliadas três medidas de segurança básicas (IG1) relacionadas a este controle (Tabela 1): 17.1 - Designar responsáveis por gerenciar o tratamento de incidentes; 17.2 - Estabelecer e manter informações de contato para reporte de incidentes de segurança; e 17.3 - Estabelecer e manter um processo para o recebimento de notificações de incidentes.

Medida de segurança 17.1 - Designar responsáveis por gerenciar o tratamento de incidentes

90.A Figura 18 traz as respostas das 377 organizações participantes à pergunta 17.1.1 do questionário: "A organização designa responsáveis por gerenciar o processo de tratamento de incidentes?". Verifica-se que quase dois terços das organizações (248) manifestaram que implementam essa prática, de algum modo (em menor parte: 52; parcialmente: 34; em maior parte ou totalmente: 162), situação que era esperada, tendo em vista se tratar da medida de segurança mais básica desse controle, sendo sua adoção, inclusive, obrigatória para os órgãos e entidades da APF, por força do Decreto 9.637/2018 (que instituiu a Política Nacional de Segurança da Informação – PNSI)[xv], art. 15, inciso VII, bem como para as empresas públicas e sociedades de economia federais que aderirem à Rede Federal de Gestão de Incidentes Cibernéticos – REGIC (Decreto 10.748/2021[xvi], art. 7º, § 2º, inciso I).

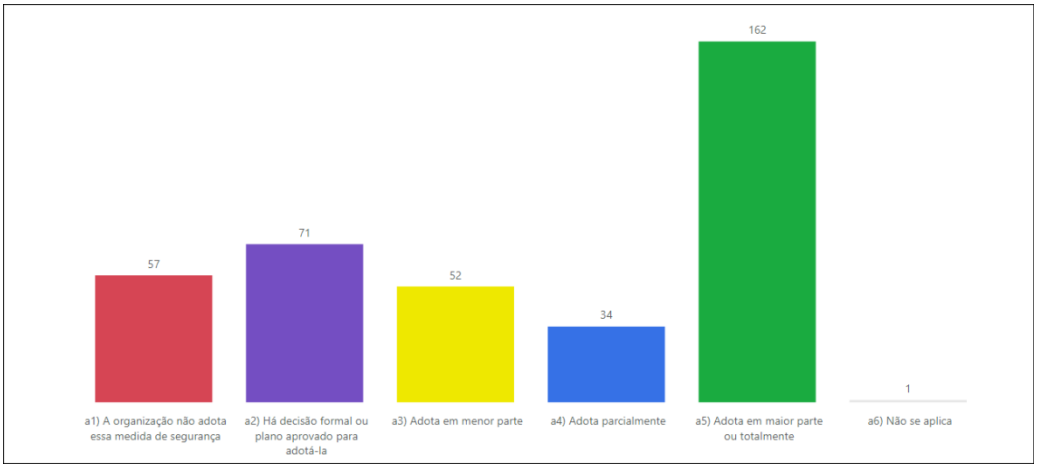



**Figura 18 - Distribuição das respostas à pergunta 17.1.1 do questionário.**
(17.1.1. A organização designa responsáveis por gerenciar o processo de tratamento de incidentes?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

91.Desconsideradas as 129 organizações que manifestaram não implementar tal medida (não adota: 57; há apenas decisão formal/plano para adotar: 71; não se aplica: 1), essas 248 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 17.1.2):

**Tabela 19 - Subpráticas da medida de segurança 17.1.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|

| | | |
|---|---|---|
| A organização designa uma pessoa chave como responsável por gerenciar o processo de tratamento de incidentes (coordenar e documentar os esforços de resposta e recuperação)? | 210 | 38 |
| Além de designar um responsável principal, a organização designa ao menos mais um substituto (*backup*), sendo que estes não podem se afastar simultaneamente? | 154 | 94 |
| A equipe de tratamento de incidentes é composta apenas por colaboradores da própria organização ou, caso possua funcionários terceirizados, todo o trabalho que esses realizam é supervisionado por ao menos um colaborador da organização? | 209 | 39 |
| As designações dos responsáveis são revisadas anualmente (ou ainda mais frequentemente)? | 64 | 184 |
| Independentemente da revisão periódica, as designações dos responsáveis são revisadas sempre que a organização passa por uma mudança significativa que pode impactar o processo de tratamento de incidentes? | 117 | 131 |

Medida de segurança 17.2 - Estabelecer e manter informações de contato para reporte de incidentes de segurança

92.A Figura 19 apresenta as respostas das 377 organizações à pergunta 17.2.1 do questionário: "A organização estabelece e mantém informações de contato para reporte de incidentes de segurança (relação com as informações de contato de todos os *stakeholders* que precisam ser informados sobre a ocorrência desses incidentes)?". Percebe-se que quase metade das organizações (178) declararam que não implementam essa medida de segurança (não adota: 100; há apenas decisão formal/plano para adotar: 77; não se aplica: 1), situação que desperta preocupação (Capítulo 3, Registro 6).

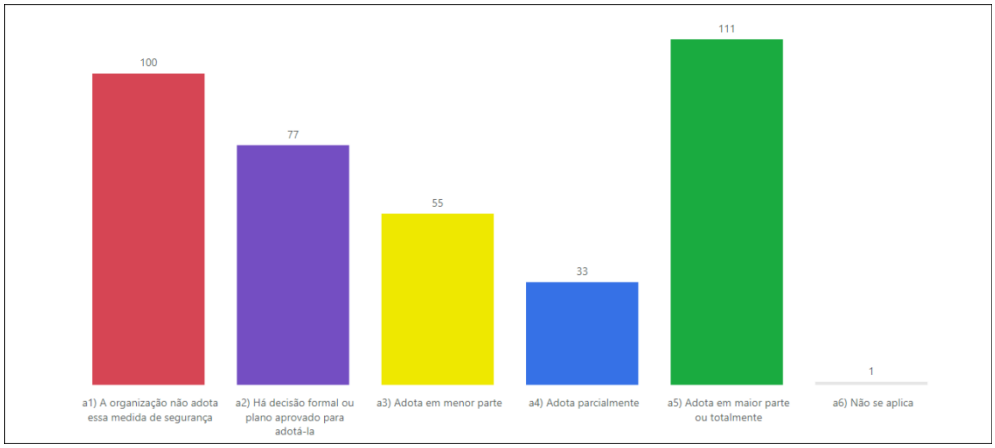



**Figura 19 - Distribuição das respostas à pergunta 17.2.1 do questionário.**
(17.2.1. A organização estabelece e mantém informações de contato para reporte de incidentes de segurança?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

93.Desconsideradas essas 178 organizações, as 199 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 17.2.2):

**Tabela 20 - Subpráticas da medida de segurança 17.2.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|

| | | |
|---|---|---|
| A relação contém as informações de contato de todos os *stakeholders* que precisam ser informados caso ocorra algum incidente de segurança (*e.g.* colaboradores internos, funcionários terceirizados, seguradoras, agentes da lei, agências/órgãos governamentais, CTIR Gov, CERT.br)? | 160 | 39 |
| A relação é comunicada periodicamente aos colaboradores que dela farão uso, frisando sua responsabilidade/obrigação de reportarem os incidentes de segurança às partes interessadas? | 86 | 113 |
| As informações de contato constantes na relação são verificadas anualmente (ou ainda mais frequentemente) para garantir que estejam sempre atualizadas? | 92 | 107 |

Medida de segurança 17.3 - Estabelecer e manter um processo para o recebimento de notificações de incidentes

94.A Figura 20, a seu turno, mostra as respostas das 377 organizações à pergunta 17.3.1 do questionário: "A organização estabelece e mantém um processo para que os colaboradores possam notificar incidentes de segurança (definindo requisitos mínimos, a exemplo dos atores, dos procedimentos, dos prazos e do conteúdo das notificações de incidentes)?". Nota-se que mais da metade das organizações (198) disseram não implementar essa medida de segurança (não adota: 100; há apenas decisão formal/plano para adotar: 96; não se aplica: 2), o que também preocupa (Capítulo 3, Registro 6).

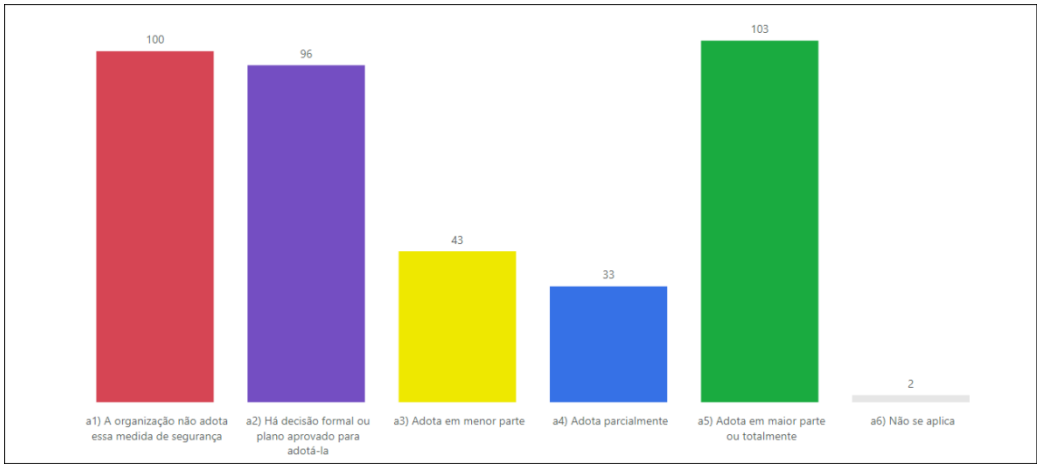



**Figura 20 - Distribuição das respostas à pergunta 17.3.1 do questionário.**
(17.3.1. A organização estabelece e mantém um processo para que os colaboradores possam notificar incidentes de segurança?)
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

95.Desconsideradas essas 198 organizações, as 179 restantes trazem o seguinte cenário em relação à implementação das subpráticas correspondentes (pergunta 17.3.2):

**Tabela 21 - Subpráticas da medida de segurança 17.3.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

| Subprática | Sim | Não |
|---|---|---|

| | | |
|---|---|---|
| O processo estabelece a responsabilidade/obrigação de os colaboradores notificarem qualquer evento de segurança da informação do qual tomem ciência e especifica o prazo para a realização da notificação, a quem a notificação deve ser encaminhada, como ela deve ser feita e quais são as informações mínimas que ela deve conter? | 115 | 64 |
| O processo é conhecido por e está à disposição de todos os colaboradores da organização? | 137 | 42 |
| O processo é revisado anualmente (ou ainda mais frequentemente)? | 55 | 124 |
| Independentemente da revisão periódica, o processo é revisado sempre que a organização passa por uma mudança significativa que pode impactá-lo? | 95 | 84 |

## 1.9. Principais desafios, deficiências e pontos de atenção apontados pelos gestores

96. Ao final, o questionário do acompanhamento oportunizou que os gestores registrassem suas percepções sobre os principais desafios, deficiências e pontos de atenção relacionados à implantação, nas suas respectivas organizações, dos controles e medidas de segurança avaliados, bem como quaisquer outras considerações que entendessem pertinentes (Anexo I, peça 855). Com isso, foram coletadas 237 respostas, cuja síntese é exposta a seguir.

97. Dentre os assuntos abordados, os principais foram recursos humanos, conscientização de usuários, treinamento e capacitação técnica, gestão e normativos de SegInfo, LGPD, orçamento e investimentos (contratações e aquisições) relacionados à infraestrutura de TI, conforme retrata a nuvem de palavras em que o tamanho dos termos ou expressões é proporcional ao número de vezes que estes foram citados nas respostas dos gestores (Figura 21).

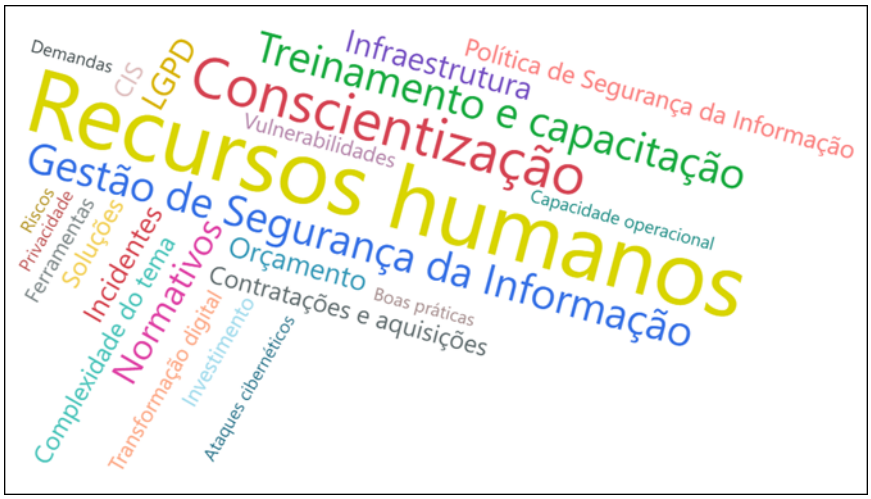



**Figura 21 - Principais desafios, deficiências e pontos de atenção apontados pelos gestores.**
(Fonte: elaboração própria, com base nas respostas dos gestores à última pergunta do questionário do acompanhamento)

98. Vários gestores reclamaram da carência de recursos humanos – em especial, de servidores efetivos – disponíveis, dedicados e capacitados em TI/SegInfo, conforme ilustram esses comentários:

> Escassez de recursos humanos do quadro de servidores dedicados à temática.
>
> Atualmente, o número de servidores são 49 e com formação em TIC apenas 2. Há uma grande rotatividade de pessoal terceirizado e estagiários (grande parte de nossos colaboradores internos).

> O principal desafio está relacionado ao número reduzido de colaboradores da gerência perante ao número de demandas e estrutura da organização. Com isso, não contamos com todo conhecimento técnico necessário.
>
> Entendo que a falta de recursos humanos seja o principal fator negativo para a falta dessas implementações. Ou seja, poucos servidores públicos na área de TI.
>
> Maior deficiência é o número de servidores com formação em TI, principalmente em segurança da informação, para acompanhar os processos desta área específica.
>
> A [organização] (...) não possui nenhum servidor efetivo especialista e dedicado para este fim. Há carência de Servidores na área de TI (...).
>
> O principal desafio é ter os recursos necessários para a publicação, adoção e execução de processos de segurança digital, onde faltam servidores que possam fazer parte dos quadros da coordenação de segurança digital (...).
>
> Temos grandes dificuldades para implementar controles efetivos em relação ao tema Segurança da Informação e Riscos. Devido à falta de recursos disponíveis, tantos recursos humanos que nos permitam desenvolver essas competências internamente quanto a falta de disponibilidade de contratação de consultoria especializadas para apoiar a instituição.
>
> Poucos servidores públicos na área de TI no órgão acaba causando sobrecarga nas atividades de gestão, atividades relacionadas a segurança da informação acabam sendo pouco priorizadas.
>
> Por fim, nosso maior desafio é atender adequadamente uma área em constante evolução e de fundamental importância para as organizações utilizando uma mão de obra insuficiente, pouco valorizada e, lamentavelmente, com tendência acentuada de perda para iniciativa privada ou mesmo para outros órgãos do governo.
>
> Baixo número de integrantes na equipe.
>
> O maior desafio é a falta de recurso humano em número suficiente para executar as funções relacionadas à TI.
>
> Um dos controles e medidas de segurança desejável para a organização seria a implantação de equipe com dedicação exclusiva à gestão da segurança da informação.

99. Outra inquietação demonstrada pelos gestores foi quanto à insuficiência de treinamento, capacitação e conscientização dos usuários de TI em relação às questões de SegInfo:

> Em que pese a realização de campanhas de conscientização sobre segurança da informação, o questionário evidenciou a necessidade de elaboração de treinamentos e/ou disponibilização de materiais a respeito do tema a todos os colaboradores de forma contínua.
>
> Os principais desafios relacionados à implantação na [organização] dos controles e medidas de segurança questionados são aqueles relacionados à absorção pelos usuários de ativos de TIC da cultura da segurança da informação decorrente da transformação digital no serviço público (...).
>
> Os desafios, no geral, provavelmente são comuns a instituições de natureza e/ou porte similares ao [da organização] e passam, entre outros, por: promover a conscientização dos colaboradores em segurança da informação, buscando ampliar o envolvimento e reforçar a importância individual para a prontidão coletiva; (...).
>
> O maior desafio a uma sensibilização mais efetiva dos servidores e colaboradores quanto [a] mecanismos de proteção de informações sensíveis relacionadas às atividades finalísticas.
>
> Dentre os requisitos de segurança da informação que é desafiador, considerados os recursos disponíveis, [na organização], consideramos a necessidade de adoção de práticas de conscientização e de treinamento de competências.
>
> Implantação da cultura de Segurança Cibernética na [organização] de maneira mais profunda.

> Ausência de plano específico para treinamento ou conscientização em segurança para os colaboradores da [organização].
>
> Fomentar a cultura de segurança da informação em todos os níveis;
>
> A principal observação é a necessidade de realizarmos treinamento de segurança para usuários finais.

a) fazer com todos compreendam a importância da Segurança da Informação e Comunicação – SIC e que apoiem a sua implementação;

100. Os gestores também manifestaram preocupação com a insuficiência de treinamento e capacitação das equipes técnicas em SegInfo/SegCiber:

> Manter e intensificar a capacitação dos recursos humanos em Segurança da Informação e Segurança Cibernética.
>
> Capacitação e ampliação da equipe de TI.
>
> Direcionamento de esforços e orçamento para capacitação contínua massiva e participação nos mais variados eventos em segurança da informação para os analistas de tecnologia da informação;
>
> Direcionamento de esforços e investimentos voltados para a criação de equipes especializadas em segurança da informação;
>
> Déficit de pessoal capacitado em Segurança de TIC.
>
> Além disto existe a necessidade de um programa de capacitação tanto dos profissionais quanto dos colaboradores devido a constante mudança que ocorre nesta área.

101. As deficiências na gestão corporativa de SegInfo também alarmam os gestores:

> A [organização] não possui setor específico de Segurança da Informação (...). Por ser uma equipe pequena, [a área de TI] termina por ser sobrecarregada com outras demandas.
>
> Outro desafio a ser destacado é escala de demandas/atividades (...) que impactam a capacidade operacional da área de Cibersegurança/Segurança da Informação.
>
> A Diretoria de Segurança da Informação não é tratada como setor estratégico da [organização];
>
> Ausência de autonomia para tomada de decisões de controles e medidas de segurança;
>
> Direcionamento de esforços e investimentos voltados para a criação de equipes especializadas em segurança da informação;
>
> O fato de a Equipe de Tratamento de Incidentes não ser uma equipe com dedicação exclusiva dificulta a implantação de controles mais efetivos para mitigação dos riscos associados à SegCiber.
>
> Destacamos como ponto de atenção a implantação da gestão de respostas a incidentes, ainda não aprovada.
>
> Ausência de estrutura de Segurança de Informação corporativa, sendo as atividades de Segurança da Informação direcionadas exclusivamente à área de TIC.
>
> Um dos controles e medidas de segurança desejável para a organização seria a implantação de equipe com dedicação exclusiva à gestão da segurança da informação.
>
> Ter uma equipe dedicada à Gestão da SIC;
>
> Como desafios, podemos citar (...) a não nomeação dos membros para composição do comitê de segurança da informação conforme recomenda a IN Nº 1 de 27 de Maio de 2020 da GSI e o Decreto 10.641/2021.

102. De igual modo, os gestores se preocupam com a ausência/insuficiência/desatualização das políticas e normativos relacionadas à área de SegInfo:

> No momento a Coordenação está trabalhando em várias frentes, contudo está focando na conformidade escrevendo políticas, normas todas em conformidade com as normas emanadas pelo GSI/PR e recomendações do TCU.
>
> Lentidão nos processos de aprovação de políticas e normas pelos conselhos gestores;
>
> Nesse momento estamos atualizando a PSI – Política de Segurança da Informação (...).
>
> Desatualização de algumas Normas de TIC e SIC.

103. Outro apontamento recorrente foi quanto à inadequação das organizações à LGPD:

> É importante destacar que [a organização] dispõe de projeto corporativo para adequação à LGPD, tendo já controles sendo adequados, governança sobre tal tema, dentre outros.
>
> [A organização] está em processo de contratação de consultoria especializada em LGPD, bem como de consultoria especializada em gestão de segurança da informação.
>
> [A organização] está com o contrato com uma consultoria para avaliação e adequação de processos e documentos à LGPD.
>
> O desafio que temos agora é de melhor empregar os quesitos quanto a segurança da informação para se adequar a LGPD.

104. Os gestores reclamaram, ainda, da insuficiência dos orçamentos destinados à área de TI e, consequentemente, dos investimentos em infraestrutura e novas tecnologias (contratações e aquisições de equipamentos, ferramentas, serviços e soluções):

> Baixo orçamento de TI em relação as necessidades [da organização], como os recursos são reduzidos as atividades relacionadas a segurança da informação acabam sendo pouco priorizadas.
>
> Outro ponto crítico é a falta de recursos para investimento em tecnologias e manutenção de sistemas legados que nos permita manter de forma controlada os riscos relativos ao tema segurança da informação.
>
> Outra dificuldade está associada a questões orçamentárias para manter o contrato com o prestador de serviço, no nosso caso o SERPRO.
>
> Vale lembrar que o nosso cenário em 2021 não mudou e continuamos com (...) necessidade de investimentos em infraestrutura, serviços e equipamentos para o bom andamento dos trabalhos.
>
> Criação de maiores rotinas de controle e aquisição de ferramentas de gestão em cibersegurança.
>
> Contratação de serviços em cibersegurança.
>
> Ausência parcial ou total de investimentos em equipamentos e novas tecnologias;
>
> Escassez de recursos financeiros destinados à área de tecnologia [da organização];
>
> Ausência de orçamento para a execução das ações de Segurança de TIC, seja de aquisição de ferramentas, terceirização, capacitação etc.
>
> Restrição de recursos financeiros para a implementação de novas tecnologias.

105. Por fim, os gestores ressaltaram a complexidade e a dinâmica dos temas (SegInfo/SegCiber) como pontos merecedores de atenção:

> Maior desafio é garantir a segurança do ambiente de TI em meio a tantos ataques cibernéticos e ao processo de transformação digital institucional (...).
>
> Nesse contexto, algo que não passou despercebido foram os diversos episódios de ataques cibernéticos aos sistemas informacionais de diversos órgãos públicos,
>
> Um outro desafio é a complexidade do tema.
>
> (...) a implementação da segurança cibernética [é um grande desafio] em um ambiente de infraestrutura tecnológica cada vez mais complexo.

Os desafios, no geral, provavelmente são comuns a instituições de natureza e/ou porte similares ao [da organização] e passam, entre outros, por: (...) promover a eficiência no processo de gestão de vulnerabilidades, considerando a complexidade e a importância crescente dos ambientes de [TI]; e evoluir os processos internos de tratamento e resposta a incidentes de segurança da informação considerando a velocidade, variedade e sofisticação crescentes dos ataques observados na Internet.

Por fim, nosso maior desafio é atender adequadamente uma área em constante evolução e de fundamental importância para as organizações (...).

[A organização] tem investido em ações que promovem cada vez mais a segurança da informação, entretanto manter e elevar o nível de controles mesmo com o aumento da complexidade das demandas de negócio e do ambiente de tecnologia da informação é desafiador.

Entendo que a parte mais desafiadora e que merece maior atenção é a parte de Gestão de Ativos, devido a quantidade e complexidade para manter todos seguros e protegidos dentro da organização. Devido a sua natureza dinâmica, constantemente novos ativos são inseridos/modificados e assim novas vulnerabilidades surgem.

## 3. Principais registros do primeiro ciclo do acompanhamento

106. Este capítulo visa a destacar os registros derivados deste primeiro ciclo do acompanhamento. Em suma, trata-se das principais conclusões decorrentes do cenário observado a partir das respostas fornecidas pelas organizações participantes da fiscalização (Capítulo 2). Além disso, apresenta sugestões de boas práticas adicionais que foram identificadas no próprio *framework* do CIS e em outras referências, como a norma ABNT NBR ISO/IEC 27002:2013.

### 3.1. Registro 1: Ativos não autorizados não estão sendo tratados

Situação encontrada

107. A Figura 22 traz os valores médios (número maior, sob o arco) e medianos (número menor, junto à linha preta) obtidos pelo conjunto das 377 organizações participantes relativamente às notas das duas medidas de segurança do controle 1, bem como o valor do indicador resultante (iControle1). Esses valores indicam que as organizações, de maneira geral, ainda estão no estágio "Inicial" de capacidade (15 < nota <= 50) em relação ao controle 1 e às correspondentes medidas de segurança (ver Tabela 22).

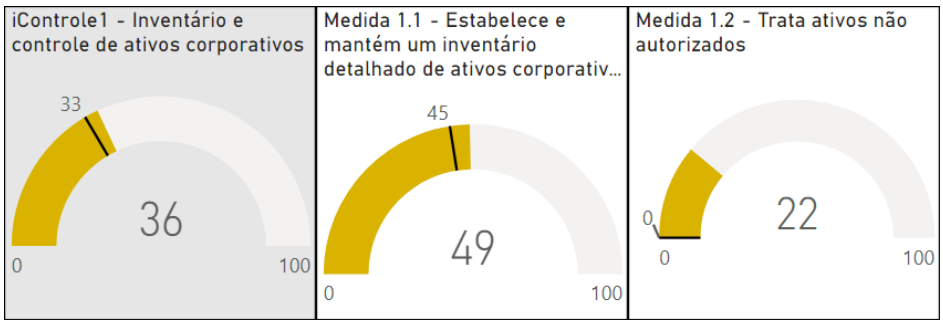



**Figura 22 - Gráficos do iControle1 e das medidas de segurança correspondentes.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

108. Em relação às duas medidas de segurança, verificou-se que 88,1% das organizações (332 de 377) mantêm algum inventário de ativos corporativos (medida 1.1; parágrafo 39), mas somente 44,3% (167 de 377) realizam algum tratamento sobre os ativos não autorizados, com o objetivo de corrigir ou remover esses dispositivos das suas redes (medida 1.2; parágrafo 42). Inclusive, como mais da metade das organizações obtiveram nota 0 nessa medida, a respectiva mediana ficou zerada (Figura 22).

109. Ademais, em termos das subpráticas relacionadas (Tabela 3), percebe-se que, das 167 organizações que implementam essa medida de segurança, até que a grande maioria remove das suas redes os dispositivos não autorizados, quando os detecta (Remove: 139; Não remove: 28). O problema é que, além de esse processo não ocorrer com a frequência adequada (Semanalmente: 43; Menos frequentemente: 124), a maioria das organizações não adota práticas mais avançadas, tais como negar futuras tentativas de conexão ao dispositivo (Nega: 53; Não nega: 114) ou mesmo colocá-lo em "quarentena" (Coloca: 28; Não coloca: 139).

Critério

110. Há uma série de normativos que remetem à necessidade de a organização identificar seus ativos de hardware, a exemplo da IN GSI/PR 3/2021, capítulo II (Mapeamento de ativos de informação), bem como das normas ABNT NBR ISO/IEC 20000-2:2008 (Tecnologia da informação – Gerenciamento de serviços – Parte 2: Código de prática), item 6.6.2 (Identificação e classificação dos ativos de informação), 27002:2013 (Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação), item 8.1.1 (Inventário dos ativos), 27005:2008 (Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação), item 8.2.1.2 (Identificação dos ativos), 27001:2006 (Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos), item 4.2.1.d.1, e ITIL v3, *Service Transition*, item 4.3 (*Service Asset and Configuration Management* – SACM).

111. A identificação desses ativos, assim como das respectivas criticidades e proprietários, é pré-requisito para que a organização possa protegê-los adequadamente. De igual modo, conforme prevê a medida de segurança 1.2 do *framework* do CIS, é consequência lógica que quaisquer ativos que não façam parte desse inventário (e que, portanto, não são ativos da organização) ou mesmo que nele estejam, mas que, por alguma razão, tenham sido configurados como não autorizados (um computador em quarentena, por exemplo), precisam ser prontamente removidos da rede ou corrigidos (ou seja, tratados).

Efeitos

112. Se a organização não é capaz de identificar e tratar equipamentos não autorizados e/ou não gerenciados na sua infraestrutura de TI, removendo-os ou corrigindo-os prontamente, estes podem ser utilizados como vetores de ataques, impactando sua segurança cibernética (*e.g.* indisponibilidade ou acesso indevido a sistemas/informações, alteração/perda de integridade de dados, violação/vazamento de informações, sobretudo pessoais/sigilosas, prejuízos financeiros, à credibilidade ou à imagem).

Boas práticas

113. Com vistas a identificar equipamentos não autorizados, além do uso tanto de ferramentas de descoberta ativa (coletam dados interagindo diretamente com os equipamentos monitorados) quanto passiva (coletam dados de *logs*, de notificações "*trap*" [*e.g. Simple Network Management Protocol* – SNMP] ou de mensagens retransmitidas pelo equipamento monitorado para um agente passivo), devem ser utilizados os *logs* (registros) do *Dynamic Host Configuration Protocol* (DHCP) para atualizar o inventário de ativos corporativos, semanalmente ou ainda mais frequentemente.

Benefícios esperados

114. A partir da identificação e do tempestivo tratamento dos ativos não autorizados e/ou não gerenciados, a organização impede que estes sejam utilizados como vetores de ataques cibernéticos, aumentando, consequentemente, sua proteção face a tais incidentes de segurança.

3.2. Registro 2: Softwares não autorizados não estão sendo tratados

Situação encontrada

115. A Figura 23 apresenta os valores médios (número maior, sob o arco) e medianos (número menor, junto à linha preta) obtidos pelo conjunto das 377 organizações relativamente ao indicador iControle2 e às notas das três medidas de segurança correspondentes. Esses valores indicam que as organizações, de modo geral, ainda estão no estágio "Inicial" de capacidade (15 < nota <= 50) em

relação ao controle 2 e a cada uma das suas três medidas de segurança correspondentes (ver Tabela 22).

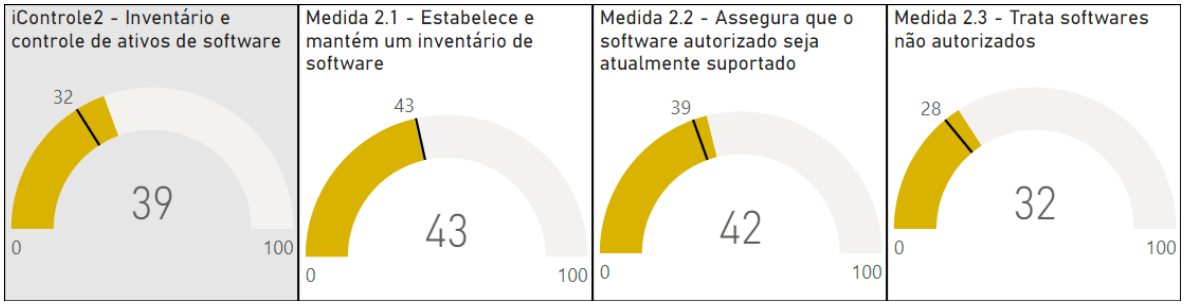



**Figura 23 - Gráficos do iControle2 e das medidas de segurança correspondentes.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

116. Em relação às três medidas de segurança, verificou-se que 71,4% das organizações (269 de 377) mantêm algum inventário de software (medida 2.1; parágrafo 49) e 70,3% (265 de 377) têm algum controle para assegurar que o software autorizado seja atualmente suportado (medida 2.2; parágrafo 51), mas somente 55,2% (208 de 377) realizam algum tratamento dos softwares não autorizados, com o objetivo de desinstalá-los dos seus ativos e/ou de bloquear a sua execução (medida 2.3; parágrafo 53).

117. Ainda, em termos das subpráticas relacionadas (Tabela 6), nota-se que, apesar de a maioria das 208 organizações que implementam essa medida de segurança possibilitar a documentação de exceções para permitir o uso de softwares não autorizados (Possibilita: 133; Não possibilita: 75) e efetivamente desinstalar softwares não autorizados para os quais não tenha sido documentada uma exceção (Desinstala: 166; Não desinstala: 42), a frequência com que esse processo de tratamento ocorre é insuficiente (Mensalmente: 42; Menos frequentemente: 166).

Critério

118. Além dos normativos mencionados no registro anterior (parágrafo 110), relativos à identificação de ativos de modo geral, o item 12.6.2 (Restrições quanto à instalação de software) da norma ABNT NBR ISO/IEC 27002:2013 especifica que "convém que sejam estabelecidas e implementadas regras definindo critérios para a instalação de software pelos usuários", tendo em vista que a instalação de softwares não autorizados pode trazer riscos a partir da introdução de vulnerabilidades que, em última análise, podem resultar em incidentes de segurança como vazamentos ou perda da integridade de dados e violações de propriedade intelectual.

119. Assim como em relação aos ativos de hardware, manter uma gerência ativa (registrar, acompanhar e corrigir) sobre os ativos de software atua para prevenir ataques, uma vez que muitos desses são possibilitados a partir da exploração de versões vulneráveis e/ou desatualizadas dos programas. Exatamente por essa razão é que a medida de segurança 2.3 do *framework* do CIS prevê que quaisquer softwares não autorizados que sejam detectados devem ser tratados, isto é, removidos (desinstalados) dos ativos, salvo se for formalmente documentada uma exceção para autorizar seu uso.

Efeitos

120. Se a organização não identifica e trata proativamente softwares não autorizados instalados e/ou rodando nos seus equipamentos, desinstalando-os, corrigindo-os ou bloqueando a sua execução, ela abre espaço para que os ativos contenham versões vulneráveis e/ou desatualizadas dos softwares, as quais podem ser utilizadas como vetores de ataques, impactando a segurança cibernética da organização.

Boas práticas

121. A documentação de exceções para permitir o uso de softwares não autorizados deve ser utilizada com bastante cautela. A partir da documentação de determinado número de exceções (ou, a depender do caso, de uma única) relacionadas ao mesmo software, convém que o setor de TI avalie a possibilidade de testá-lo e homologá-lo, de modo que este deixe de possuir o *status* de exceção e passe a integrar o rol dos softwares efetivamente autorizados.

122. Ademais, salvo em organizações muito pequenas (e, consequentemente, com poucas máquinas), faz-se necessário tanto utilizar ferramentas que automatizem o processo de descoberta e documentação (inventário) dos softwares presentes quanto implementar controles técnicos (listas de permissões, assinaturas digitais, controle de versão), a serem periodicamente avaliados, com vistas a garantir que apenas aplicações, bibliotecas (arquivos .dll, .ocx, .so etc.) e/ou *scripts* (arquivos .ps1, .py etc.) específicos possam ser executados, acessados ou carregados em processos do sistema.

Benefícios esperados

123. A partir da identificação e do tempestivo tratamento dos softwares não autorizados (e para os quais não tenha sido documentada uma exceção), a organização impede que estes sejam utilizados como vetores de ataques, aumentando sua resiliência cibernética.

### 3.3. Registro 3: Deficiências nos processos de gestão e de correção de vulnerabilidades

Situação encontrada

124. A Figura 24 mostra os valores médios (números maiores) e medianos (números menores) do conjunto das 377 organizações em relação ao indicador iControle7 e às notas das respectivas quatro medidas de segurança. Esses valores indicam que as organizações, de modo geral, ainda estão no estágio "Inicial" de capacidade (15 < nota <= 50) em relação ao controle 7 e às medidas de segurança 7.1, 7.2 e 7.4, sendo que apenas na medida 7.3 já alcançaram o estágio "Intermediário" (ver Tabela 22).

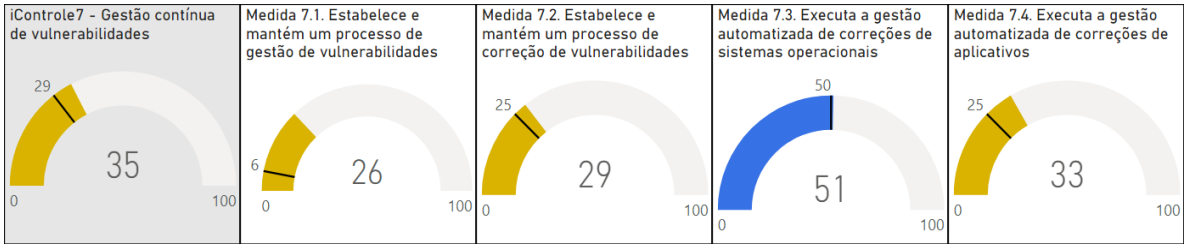



**Figura 24 - Gráficos do iControle7 e das medidas de segurança correspondentes.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

125. Em relação às quatro medidas de segurança, verificou-se que 57% das organizações (215 de 377) ainda não estabeleceram um processo de gestão de vulnerabilidades (medida 7.1; parágrafo 58), 46,7% (176 de 377) ainda não estabeleceram um processo de correção (medida 7.2; parágrafo 60) e 39,8% (150 de 377) não executam a gestão automatizada das correções em aplicativos (medida 7.4; parágrafo 64), ao passo que 77,2% (291 de 377) fazem a gestão automatizada das correções em sistemas operacionais (medida 7.3; parágrafo 63), atuando para detectar e corrigir as vulnerabilidades nesses softwares antes que eventuais atacantes tenham oportunidade de explorá-las (ver Registro 4).

126. Quanto às subpráticas relacionadas à gestão de vulnerabilidades (Tabela 7), apesar de a maioria das 162 organizações que implementam essa medida de segurança ter documentado o processo (Documentou: 106; Não documentou: 56) e promover sua atualização sempre que a organização passa por uma mudança significativa que pode impactá-lo (Atualiza: 85; Não atualiza: 77), uma minoria aprovou formalmente o processo (Aprovou: 60; Não aprovou: 102), definiu os papéis e responsabilidades associados (Definiu: 65; Não definiu: 97) e promove sua revisão e atualização com periodicidade adequada (Anualmente: 41; Menos frequentemente: 121).

127. A seu turno, no que diz respeito às subpráticas relativas à correção de vulnerabilidades (Tabela 8), apesar de a grande maioria das 201 organizações que implementam essa medida priorizar a correção das vulnerabilidades identificadas (Prioriza: 167; Não prioriza: 34), a minoria documentou o processo (Documentou: 81; Não documentou: 120), aprovou-o formalmente (Aprovou: 57; Não aprovou: 144) e promove a análise e revisão das vulnerabilidades e riscos associados com suficiente periodicidade (Mensalmente: 68; Menos frequentemente: 133).

Critério

128. Conforme o item 12.6.1 (Gestão de vulnerabilidades técnicas) da norma ABNT NBR ISO/IEC 27002:2013, "convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso [pela organização] sejam obtidas em tempo hábil", que a exposição a elas "seja avaliada e que sejam tomadas as medidas apropriadas para lidar com os riscos associados".

129. Adicionalmente, as medidas de segurança 7.1 e 7.2 do *framework* do CIS, respectivamente, preveem o estabelecimento e a manutenção de processos de gestão e de correção de vulnerabilidades.

Efeitos

130. Se a organização não implementa e executa continuamente tais processos (gestão e correção de vulnerabilidades), acaba por fornecer aos potenciais atacantes longas janelas de oportunidade para a perpetração de ataques que visem a explorar ameaças e vulnerabilidades conhecidas.

Boas práticas

131. Os processos de gestão e de correção de vulnerabilidades podem ser vistos como subfunções do processo de gestão de mudanças da organização e, portanto, podem aproveitar as práticas e procedimentos associados, a exemplo dos itens 12.1.2 (Gestão de mudanças) e 14.2.2 (Procedimentos para controle de mudanças de sistemas) da norma ABNT NBR ISO/IEC 27002:2013 e da *Information Technology Infrastructure Library* (ITIL) v3, *Service Transition*, item 4.2 (*Change Management*).

132. Salvo em organizações pequenas (e com poucos equipamentos), faz-se necessário utilizar ferramentas que permitam automatizar a realização das varreduras de vulnerabilidades (que devem incluir os ativos internos da organização e aqueles expostos externamente e devem ser completas, tanto autenticadas quanto não autenticadas), bem como a respectiva correção, sempre que possível. Preferencialmente, tais ferramentas devem adotar definições padronizadas, baseadas no *Security Content Automation Protocol* (SCAP).

Benefícios esperados

133. A partir da realização contínua dos processos de gestão e de correção de vulnerabilidades, a organização se torna proativa na detecção, acompanhamento e correção de ameaças e riscos conhecidos em seus ativos de TI, impedindo sua exploração por atacantes e melhorando sua defesa cibernética.

3.4. Registro 4 [POSITIVO]: A gestão automatizada de correções de SOs está sendo executada

Situação encontrada

134. Das 377 organizações, 77,2% (291) estão executando, em alguma medida, a gestão automatizada das correções de sistemas operacionais (Figura 24, medida 7.3; parágrafo 63), o que atua para aumentar a tempestividade da aplicação desses *patches* e, consequentemente, diminuir a janela de oportunidade que eventuais atacantes possuem para explorar vulnerabilidades nesses ativos.

135. Conforme mostra a Tabela 9, apesar de apenas metade dessas 291 organizações testarem os *patches* antes da sua instalação (Testam: 147; Não testam: 144), a maioria realiza o processo de verificação da existência dessas correções com suficiente frequência (Mensalmente: 171; Menos frequentemente: 120) e a grande maioria utiliza ferramentas automatizadas para conduzir esse

processo (Automatiza: 227; Não automatiza: 64) e monitora fontes públicas e privadas de informações para identificar ameaças, vulnerabilidades e medidas mitigatórias (Monitoram: 207; Não monitoram: 84).

Critério

136. Conforme o item 12.6.1 (Gestão de vulnerabilidades técnicas) da norma ABNT NBR ISO/IEC 27002:2013, "convém que informações sobre vulnerabilidades técnicas dos sistemas de informação em uso [pela organização] sejam obtidas em tempo hábil", que a exposição a elas "seja avaliada e que sejam tomadas as medidas apropriadas para lidar com os riscos associados".

137. Ademais, a medida de segurança 7.3 do *framework* do CIS prevê a automatização da gestão da aplicação de correções (*patches*) de sistemas operacionais.

Efeitos

138. Se a organização não automatiza o processo de aplicação de *patches* de segurança nos seus sistemas operacionais, acaba por não corrigir tempestivamente ameaças e vulnerabilidades conhecidas, fornecendo aos potenciais atacantes longas janelas de oportunidade para sua exploração.

Boas práticas

139. Tendo em vista que os fornecedores estão sendo pressionados a liberarem seus pacotes de correções (*patches*) com cada vez mais brevidade, é muito importante, antes da respectiva aplicação, realizar testes tanto para atestar que o problema em questão será adequadamente resolvido quanto para garantir que não serão causados efeitos colaterais indesejáveis. Isso porque, em determinados casos, pode ser bem complicado ou até inviável desinstalar uma correção após sua instalação, ocasionando um prejuízo ainda maior do que o problema inicial e podendo até impactar a continuidade do negócio (norma ABNT NBR ISO/IEC 27031:2015 – Tecnologia da informação – Técnicas de segurança – Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação).

140. Se a organização não tiver condições de conduzir tais testes de maneira satisfatória por conta própria, deve avaliar a conveniência e a oportunidade de atrasar a aplicação da correção de modo a avaliar os riscos associados a partir das experiências relatadas por outros usuários/organizações.

Benefícios esperados

141. A partir da automatização do processo de aplicação de correções (*patches*), ameaças e vulnerabilidades conhecidas são corrigidas tempestivamente, impedindo que sejam exploradas por possíveis atacantes e, portanto, diminuindo a superfície de ataque da organização.

3.5. Registro 5: Conscientização e treinamento deficientes

Situação encontrada

142. A Figura 25 mostra os valores médios (números maiores) e medianos (números menores) das 377 organizações em relação ao indicador iControle14 e às notas das respectivas oito medidas de segurança. Esses valores indicam que as organizações, de modo geral, ainda estão no estágio "Inicial" de capacidade (15 < nota <= 50) em relação ao controle 14 e a todas as suas medidas de segurança básicas, à exceção da medida 14.7, que está ainda pior (ainda no estágio "Inexpressivo" - ver Tabela 22).

143. Percebe-se, então, que há nítida deficiência em todas as medidas de segurança relativas à conscientização e ao treinamento dos colaboradores, em especial para identificarem e notificarem a falta de atualizações de segurança nos ativos (medida 14.7) e para conhecerem os riscos relacionados a redes inseguras (medida 14.8), nas quais a mediana ficou zerada porque mais da metade das organizações obtiveram nota 0 em relação a tais medidas (Figura 25).

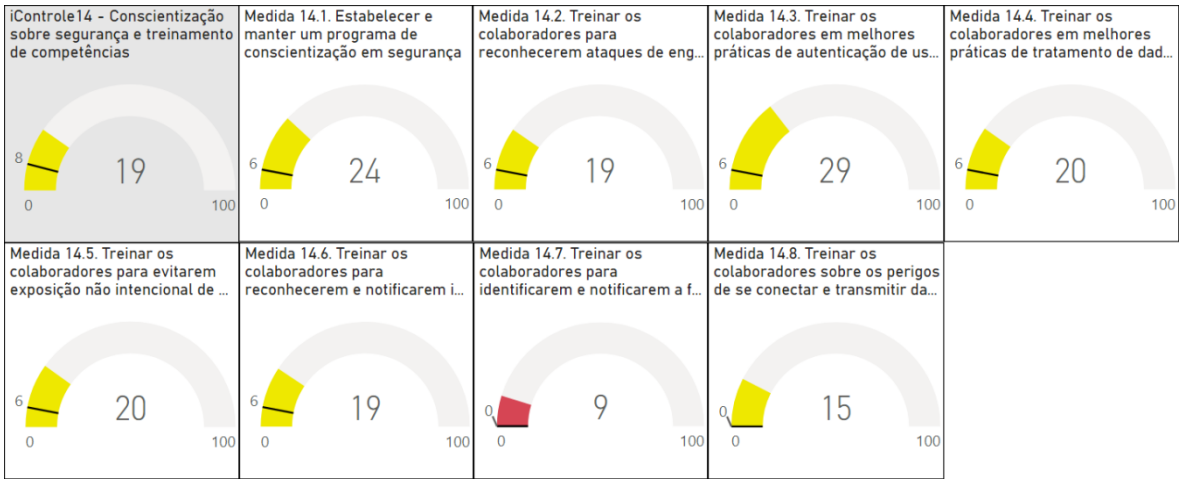



**Figura 25 - Gráficos do iControle14 e das medidas de segurança correspondentes.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

144. Mesmo entre as organizações que disseram implementar (em menor parte, parcialmente ou mesmo em maior parte/totalmente) as medidas de segurança associadas, algumas carências relacionadas a determinadas subpráticas preocupam. Por exemplo, poucas organizações treinam seus colaboradores em requisitos específicos de segurança antes de estes assumirem novos cargos (Treinam: 20; Não treinam: 138) [Tabela 11]. A capacitação em engenharia social também é insuficiente: menos da metade das organizações abordam as técnicas de pretexto (Abordam: 55; Não abordam: 83) e de "isca" (Abordam: 54; Não abordam: 84) e muito poucas abordam ataques dos tipos quiproquó (Abordam: 27; Não abordam: 111) ou "carona" (Abordam: 29; Não abordam: 109) [Tabela 12]. Explicações sobre essas técnicas e ataques podem ser encontradas no **Error! Reference source not found.**.

145. Ademais, poucos treinamentos abordam aspectos relativos à deleção permanente de arquivos e dados e ao descarte seguro de mídias/equipamentos (Abordam: 36; Não abordam: 82) [Tabela 14] ou aos sinais precursores e indicadores da ocorrência de incidentes de segurança (Abordam: 37; Não abordam: 77), tampouco ensinam os colaboradores a terem noção do tipo, da extensão e da magnitude do problema em incidentes (Ensinam: 41; Não ensinam: 73) [Tabela 16] ou mesmo sobre as diferenças entre os protocolos de criptografia de redes wi-fi (Ensinam: 10; Não ensinam: 82) [Tabela 18].

Critério

146. Conforme o item 7.2.2 (Conscientização, educação e treinamento em segurança da informação) da norma ABNT NBR ISO/IEC 27002:2013, "convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções".

147. A seu turno, de acordo com o item 5.1 da NC 18/IN01/DSIC/GSIPR (Diretrizes para as atividades de ensino em Segurança da Informação e Comunicações [SIC] nos órgãos e entidades da Administração Pública Federal [APF]): "os Agentes Públicos deverão receber orientações/instruções em [SIC] no período de ambientação, formação inicial ou continuada em seus órgãos ou entidades, por meio de atividades de ensino de sensibilização, conscientização, capacitação e especialização".

148. Adicionalmente, todas as medidas do controle 14 (*Security Awareness and Skills Training*) do *framework* do CIS preveem o estabelecimento e a manutenção de um programa contínuo e permanente de conscientização e treinamento dos colaboradores em segurança (da informação e cibernética), de modo a fazer com que adotem comportamentos e procedimentos mais seguros.

Efeitos

149. Se a organização não implementa um programa adequado de conscientização e treinamento em segurança (da informação e cibernética), seus colaboradores não terão os conhecimentos e as habilidades necessários para adotarem rotinas e procedimentos seguros ao realizarem suas tarefas de trabalho, ocasionando vulnerabilidades derivadas do comportamento humano, as quais poderão ser exploradas por atacantes, prejudicando a organização.

Boas práticas

150. Os programas de conscientização e treinamento não devem se restringir ao ensino de "o que" e "como" fazer, mas, sobretudo, devem explicar aos colaboradores as razões ("por que") por trás de cada uma das questões de segurança abordadas e mostrar-lhes os objetivos da SegInfo e os impactos potenciais, positivos e negativos, dos seus diferentes comportamentos e condutas sobre a organização.

151. Ademais, é sempre importante testar os conhecimentos adquiridos pelos colaboradores ao final da realização de quaisquer ações de conscientização, educação e/ou treinamento em segurança (da informação e cibernética), as quais podem fazer parte de atividades educacionais de TI mais abrangentes ou, ainda, de outros treinamentos e cursos de caráter mais geral em segurança.

Benefícios esperados

152. A partir do estabelecimento e manutenção de um programa contínuo e permanente de conscientização e treinamento dos colaboradores em segurança, estes passam a ter conhecimentos e habilidades suficientes para adotarem comportamentos e procedimentos mais seguros na realização das suas tarefas e rotinas de trabalho cotidianas, dando menos margem à exploração de vulnerabilidades derivadas do comportamento humano e, assim, aumentando a segurança cibernética da organização.

3.6. Registro 6: Processo de gestão de resposta a incidentes de segurança deficiente

Situação encontrada

153. A Figura 26 mostra os valores médios (números maiores) e medianos (números menores) das 377 organizações em relação ao indicador iControle17 e às notas das respectivas três medidas de segurança. Esses valores indicam que as organizações, de modo geral, ainda estão no estágio "Inicial" de capacidade (15 < nota <= 50) em relação ao controle 17 e às suas práticas (ver Tabela 22).

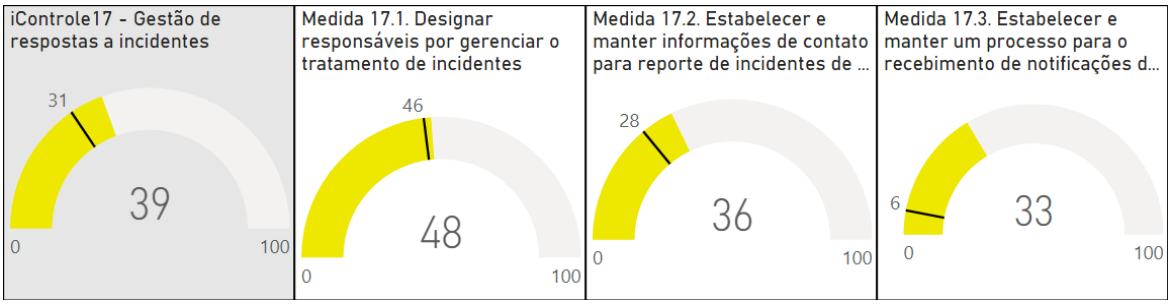



**Figura 26 - Gráficos do iControle17 e das medidas de segurança correspondentes.**
(Fonte: painel construído para visualizar as respostas das organizações [Capítulo 4])

154. Em relação às três medidas de segurança, verificou-se que 65,8% das organizações (248 de 377) designaram algum responsável por gerenciar o tratamento de incidentes de segurança (medida 17.1; parágrafo 90), 52,8% (199 de 377) mantêm informações de contato para o reporte desses incidentes (medida 17.2; parágrafo 93) e 47,5% (179 de 377) estabeleceram alguma parte do processo para o recebimento de notificações de incidentes (medida 17.3; parágrafo 95)

155. Ademais, em termos das subpráticas relacionadas a essas três medidas, verificou-se que: i) das 248 organizações que designam responsável por gerenciar o tratamento de incidentes de segurança (medida 17.1; Tabela 19), a maioria não revisa essa designação com frequência adequada

(Anualmente: apenas 64; Menos frequentemente: 184); ii) das 199 organizações que mantêm informações de contato para reporte de incidentes (medida 17.2; Tabela 20), menos da metade verifica essas informações com frequência adequada (Anualmente: 92; Menos frequentemente: 107); e iii) das 179 organizações que implementam o recebimento de notificações de incidentes (medida 17.3; Tabela 21), a maioria não revisa esse processo com frequência adequada (Anualmente: apenas 55; Menos frequentemente: 124).

Critério

156. De acordo com o item 16.1.5 (Resposta aos incidentes de segurança da informação) da norma ABNT NBR ISO/IEC 27002:2013, "convém que incidentes de segurança da informação sejam reportados de acordo com procedimentos documentados". As diretrizes para implementação desse item trazem uma série de requisitos a serem atendidos pelas notificações de incidentes.

157. Ainda, conforme o item 8.1 da NC 8/IN01/DSIC/GSIPR (Gestão de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais [ETIR]: diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal [APF]): "Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR".

158. Por fim, a medida de segurança 17.3 do *framework* do CIS também menciona requisitos que as notificações de incidentes devem conter, a exemplo do prazo para sua realização, a quem devem ser encaminhadas, como devem ser feitas e seu conteúdo mínimo.

Efeitos

159. Se a organização não estabelece e mantém um processo padronizado para o recebimento de notificações de incidentes de segurança, a gestão de respostas a incidentes fica seriamente prejudicada, não ocorrendo, portanto, a pronta detecção e resposta em relação a ataques e ameaças potenciais e reais, com impactos negativos na segurança cibernética da organização.

Boas práticas

160. A equipe de resposta a incidentes deve realizar treinamento periódico baseado em cenários de ataque (ajustados para as ameaças e impactos potenciais enfrentados pela organização), pois esses ajudam a garantir que tanto a liderança corporativa quanto os membros da equipe técnica tenham plena ciência e estejam sempre preparados para desempenhar suas funções no processo de resposta. Esses treinamentos também contribuem para a identificação de lacunas nos planos e processos de resposta, bem como de dependências inesperadas, ajudando a promover, assim, sua atualização constante.

161. Organizações mais maduras devem incluir inteligência sobre ameaças no seu processo de resposta a incidentes, tornando sua equipe mais proativa a partir do desenvolvimento da capacidade de identificar atacantes chave para a organização (ou seu segmento de atuação), bem como de pesquisar e monitorar as respectivas táticas, técnicas e procedimentos operacionais (*Tactics, Techniques, and Procedures* – TTP). Essa prática ajudará a focar as detecções e a definir procedimentos de resposta mais rápidos para identificar e corrigir incidentes de segurança.

Benefícios esperados

162. A partir do estabelecimento e da cobrança de requisitos para as notificações (obrigação de os colaboradores notificarem incidentes, prazo para notificar, destinatário, canais, conteúdo mínimo etc.), a organização melhora sua capacidade de identificar potenciais ataques e ameaças, responder a elas antes que se espalhem, corrigi-las antes que causem prejuízos e recuperar dados e sistemas eventualmente corrompidos, tonando-se, assim, mais resiliente.

3.7. Evidências, análises, causas e encaminhamentos dos registros

163. Como essas seções acabariam sendo muito parecidas para todos os registros, considerou-se preferível apresentá-las de modo unificado, ao final, do que as repetir dentro da estrutura de cada um.

164. As evidências que suportam os registros derivam das respostas ao questionário do acompanhamento, fornecidas pelos gestores designados pelas 377 organizações participantes. As respectivas análises foram inseridas na seção "Situação encontrada" de cada registro.

165. À exceção do registro positivo (Registro 4), os demais têm por causa a imaturidade das organizações quanto à gestão de SegInfo, que acaba ocasionando a não implementação das medidas de segurança e subpráticas questionadas. Esse quadro é agravado pela ausência, de modo geral, de normativos que orientem e direcionem os gestores no que tange à implementação desses controles.

166. 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 Levantamento Integrado de Governança Organizacional Pública de 2018 [TC 015.268/2018-7]), e o iSegCiber, indicador criado neste acompanhamento para aferir o nível geral de adoção dos controles críticos verificados (Figura 35).

167. Assim, considerando que, em maior ou menor grau, os registros compartilham essa mesma causa (imaturidade em gestão de SegInfo), os encaminhamentos buscam, em essência, atenuar essa deficiência. Com esse intuito, propõe-se recomendar aos Órgãos Governantes Superiores (OGS) dos Poderes Executivo e Judiciário que editem normativos para endereçar as questões abordadas neste relatório em relação às entidades e órgãos públicos sob os seus respectivos âmbitos de jurisdição administrativa. Recomendações semelhantes também serão propostas ao Senado Federal, à Câmara dos Deputados, ao Tribunal de Contas da União, ao Supremo Tribunal Federal e ao Ministério Público da União.

## 4. Painel para visualização gráfica das respostas fornecidas pelas organizações

168. Esta fiscalização incluiu a construção de um painel (*dashboard*) – utilizando a ferramenta Microsoft Power BI – para permitir a visualização gráfica e interativa das informações fornecidas pelas organizações auditadas em resposta ao questionário deste primeiro ciclo do acompanhamento de controles críticos de SegCiber. Ressalva-se que, por conter informações sigilosas, o acesso ao painel ficou restrito à equipe de auditores da Sefti.

169. Além de mostrar a situação observada neste primeiro ciclo, o painel será utilizado para possibilitar que o TCU continue acompanhando de modo efetivo a implementação dos controles críticos de SegCiber por parte das organizações públicas federais.

170. O painel foi estruturado em quatro abas descritivas ("Introdução", "Indicadores", "Controles" e "Outros indicadores") e em dez abas de visualização de dados: "Indicadores - resultados", "Controle 1", "Controle 2", "Controle 7", "Controle 14", "Controle 17", "nSegCiber X iBackup", "nSegInfo X iSegCiber", "Radar" e "Lista das organizações".

171. Os gráficos de todas as abas de visualização de dados são dinâmicos, o que significa que o universo dos dados apresentados pode ser alterado com base na aplicação dos filtros disponíveis (Figura 27), 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.

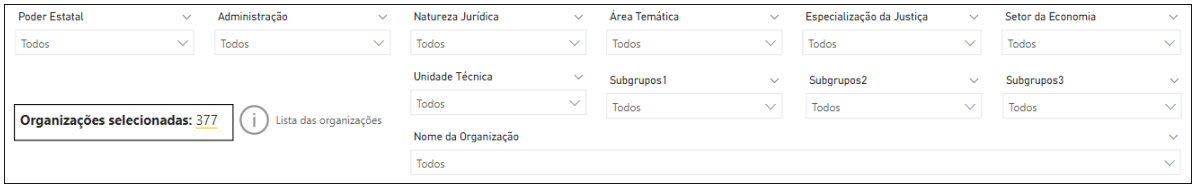



**Figura 27 - Painel "Acompanhamento de controles críticos de SegCiber" - Filtros disponíveis.**
(Fonte: painel construído para visualizar as respostas das organizações)

172. As opções possíveis dos filtros disponíveis são:

172.1. Poder Estatal: “Executivo”, “Função Essencial à Justiça”, “Judiciário”, “Legislativo” e “Paraestatal”;

172.2. Administração: “Direta”, “Indireta” e “Paraestatal”;

172.3. Natureza Jurídica: “Autarquia”, “Empresa Pública”, “Fundação”, “Órgão Público”, “Serviço Social Autônomo” e “Sociedade de Economia Mista”;

172.4. Área Temática: “Agência Reguladora”, “Banco”, “Casa Legislativa”, “Conselho Profissional”, “Instituição de ensino”, “Militar”, “Ministério”, “Ministério Público”, “Não se aplica”, “Outra”, “Segurança Pública”, “Sistema S”, “Tribunal de Contas”, “Tribunal do Judiciário” e “Unidade de Saúde”;

172.5. Especialização da Justiça: “Justiça do Distrito Federal e Territórios”, “Justiça do Trabalho”, “Justiça Eleitoral”, “Justiça Federal”, “Justiça Militar” e “Não se aplica”;

172.6. Setor da Economia: “Abastecimento”, “Comércio e Serviços”, “Comunicações”, “Desenvolvimento Regional”, “Energia”, “Financeiro”, “Indústria de Transformação”, “Não se aplica”, “Pesquisa, desenvolvimento e planejamento”, “Petróleo, gás e derivados”, “Portuário”, “Saúde”, “Seguros” e “Transportes”;

172.7. Unidade Técnica: “SecexAdministração”, “SecexAgroAmbiental”, “SecexDefesa”, “SecexDesenvolvimento”, “SecexEducação”, “SecexFinanças”, “SecexPrevidência”, “SecexSaúde”, “SecexTributária”, “Sefti”, “SeinfraCOM”, “SeinfraElétrica”, “SeinfraPetróleo”, “SeinfraPortoFerrovia”, “SeinfraRodoviaAviação”, “SeinfraUrbana” e “Semag” (clientela das unidades técnicas do TCU);

172.8. Subgrupos1, Subgrupos2 e Subgrupos3: três filtros que foram configurados com subgrupos de organizações similares (**Error! Reference source not found.**), de modo que se possa visualizar como estão quando comparadas entre si;

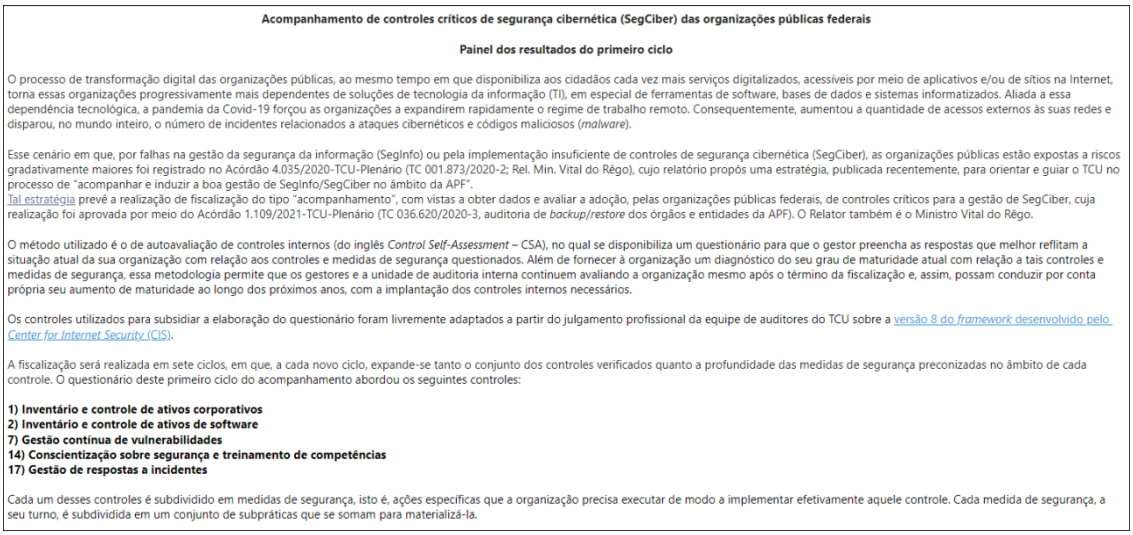
172.9. Nome da organização: nome das 377 organizações avaliadas.

173. A partir da aplicação dos filtros descritos, as respostas das organizações participantes podem ser visualizadas e comparadas com base em diversos critérios distintos, permitindo, assim, ampla segmentação das análises. Esses filtros, inclusive, serão usados para gerar os gráficos que ilustrarão os relatórios comparativos de *feedback* a serem enviados às organizações (parágrafo 200198).

174. A seguir, as abas são descritas segundo a ordem em que aparecem no painel, sendo que os gráficos mostram os dados completos, sem a aplicação dos filtros.

Aba “Introdução”

175. Essa aba descreve a fiscalização e o método utilizado (CSA), além de enumerar os cinco controles avaliados (Figura 28).



**Acompanhamento de controles críticos de segurança cibernética (SegCiber) das organizações públicas federais**

**Painel dos resultados do primeiro ciclo**

O processo de transformação digital das organizações públicas, ao mesmo tempo em que disponibiliza aos cidadãos cada vez mais serviços digitalizados, acessíveis por meio de aplicativos e/ou de sítios na Internet, torna essas organizações progressivamente mais dependentes de soluções de tecnologia da informação (TI), em especial de ferramentas de software, bases de dados e sistemas informatizados. Aliada a essa dependência tecnológica, a pandemia da Covid-19 forçou as organizações a expandirem rapidamente o regime de trabalho remoto. Consequentemente, aumentou a quantidade de acessos externos às suas redes e disparou, no mundo inteiro, o número de incidentes relacionados a ataques cibernéticos e códigos maliciosos (*malware*).

Esse cenário em que, por falhas na gestão da segurança da informação (SegInfo) ou pela implementação insuficiente de controles de segurança cibernética (SegCiber), as organizações públicas estão expostas a riscos gradativamente maiores foi registrado no Acórdão 4.035/2020-TCU-Plenário (TC 001.873/2020-2; Rel. Min. Vital do Rêgo), cujo relatório propôs uma estratégia, publicada recentemente, para orientar e guiar o TCU no processo de "acompanhar e induzir a boa gestão de SegInfo/SegCiber no âmbito da APF".
Tal estratégia prevê a realização de fiscalização do tipo "acompanhamento", com vistas a obter dados e avaliar a adoção, pelas organizações públicas federais, de controles críticos para a gestão de SegCiber, cuja realização foi aprovada por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de *backup/restore* dos órgãos e entidades da APF). O Relator também é o Ministro Vital do Rêgo.

O método utilizado é o de autoavaliação de controles internos (do inglês *Control Self-Assessment* – CSA), no qual se disponibiliza um questionário para que o gestor preencha as respostas que melhor reflitam a situação atual da sua organização com relação aos controles e medidas de segurança questionados. Além de fornecer à organização um diagnóstico do seu grau de maturidade atual com relação a tais controles e medidas de segurança, essa metodologia permite que os gestores e a unidade de auditoria interna continuem avaliando a organização mesmo após o término da fiscalização e, assim, possam conduzir por conta própria seu aumento de maturidade ao longo dos próximos anos, com a implantação dos controles internos necessários.

Os controles utilizados para subsidiar a elaboração do questionário foram livremente adaptados a partir do julgamento profissional da equipe de auditores do TCU sobre a versão 8 do *framework* desenvolvido pelo *Center for Internet Security* (CIS).

A fiscalização será realizada em sete ciclos, em que, a cada novo ciclo, expande-se tanto o conjunto dos controles verificados quanto a profundidade das medidas de segurança preconizadas no âmbito de cada controle. O questionário deste primeiro ciclo do acompanhamento abordou os seguintes controles:

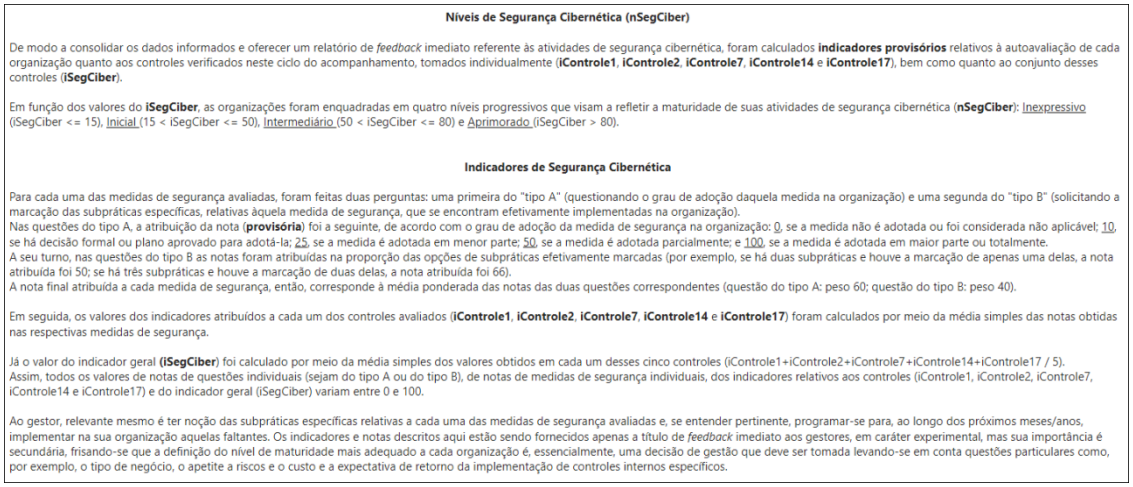
**1) Inventário e controle de ativos corporativos**
**2) Inventário e controle de ativos de software**
**7) Gestão contínua de vulnerabilidades**
**14) Conscientização sobre segurança e treinamento de competências**
**17) Gestão de respostas a incidentes**

Cada um desses controles é subdividido em medidas de segurança, isto é, ações específicas que a organização precisa executar de modo a implementar efetivamente aquele controle. Cada medida de segurança, a seu turno, é subdividida em um conjunto de subpráticas que se somam para materializá-la.

**Figura 28 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Introdução".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Indicadores"

176. Essa aba traz uma descrição sucinta dos indicadores que foram calculados com base nas respostas das organizações avaliadas (Figura 29).



**Níveis de Segurança Cibernética (nSegCiber)**

De modo a consolidar os dados informados e oferecer um relatório de *feedback* imediato referente às atividades de segurança cibernética, foram calculados **indicadores provisórios** relativos à autoavaliação de cada organização quanto aos controles verificados neste ciclo do acompanhamento, tomados individualmente (**iControle1**, **iControle2**, **iControle7**, **iControle14** e **iControle17**), bem como quanto ao conjunto desses controles (**iSegCiber**).

Em função dos valores do **iSegCiber**, as organizações foram enquadradas em quatro níveis progressivos que visam a refletir a maturidade de suas atividades de segurança cibernética (**nSegCiber**): Inexpressivo (iSegCiber <= 15), Inicial (15 < iSegCiber <= 50), Intermediário (50 < iSegCiber <= 80) e Aprimorado (iSegCiber > 80).

**Indicadores de Segurança Cibernética**

Para cada uma das medidas de segurança avaliadas, foram feitas duas perguntas: uma primeira do "tipo A" (questionando o grau de adoção daquela medida na organização) e uma segunda do "tipo B" (solicitando a marcação das subpráticas específicas, relativas àquela medida de segurança, que se encontram efetivamente implementadas na organização).
Nas questões do tipo A, a atribuição da nota (**provisória**) foi a seguinte, de acordo com o grau de adoção da medida de segurança na organização: 0, se a medida não é adotada ou foi considerada não aplicável; 10, se há decisão formal ou plano aprovado para adotá-la; 25, se a medida é adotada em menor parte; 50, se a medida é adotada parcialmente; e 100, se a medida é adotada em maior parte ou totalmente.
A seu turno, nas questões do tipo B as notas foram atribuídas na proporção das opções de subpráticas efetivamente marcadas (por exemplo, se há duas subpráticas e houve a marcação de apenas uma delas, a nota atribuída foi 50; se há três subpráticas e houve a marcação de duas delas, a nota atribuída foi 66).
A nota final atribuída a cada medida de segurança, então, corresponde à média ponderada das notas das duas questões correspondentes (questão do tipo A: peso 60; questão do tipo B: peso 40).

Em seguida, os valores dos indicadores atribuídos a cada um dos controles avaliados (**iControle1**, **iControle2**, **iControle7**, **iControle14** e **iControle17**) foram calculados por meio da média simples das notas obtidas nas respectivas medidas de segurança.

Já o valor do indicador geral (**iSegCiber**) foi calculado por meio da média simples dos valores obtidos em cada um desses cinco controles (iControle1+iControle2+iControle7+iControle14+iControle17 / 5).
Assim, todos os valores de notas de questões individuais (sejam do tipo A ou do tipo B), de notas de medidas de segurança individuais, dos indicadores relativos aos controles (iControle1, iControle2, iControle7, iControle14 e iControle17) e do indicador geral (iSegCiber) variam entre 0 e 100.

Ao gestor, relevante mesmo é ter noção das subpráticas específicas relativas a cada uma das medidas de segurança avaliadas e, se entender pertinente, programar-se para, ao longo dos próximos meses/anos, implementar na sua organização aquelas faltantes. Os indicadores e notas descritos aqui estão sendo fornecidos apenas a título de *feedback* imediato aos gestores, em caráter experimental, mas sua importância é secundária, frisando-se que a definição do nível de maturidade mais adequado a cada organização é, essencialmente, uma decisão de gestão que deve ser tomada levando-se em conta questões particulares como, por exemplo, o tipo de negócio, o apetite a riscos e o custo e a expectativa de retorno da implementação de controles internos específicos.

**Figura 29 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Indicadores".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Indicadores - resultados"

177. Essa aba apresenta um gráfico com a distribuição das organizações avaliadas em função dos níveis de maturidade em SegCiber definidos no âmbito do acompanhamento (Tabela 22), bem como outros seis gráficos com os valores médios (número maior, sob o arco) e medianos (número menor, junto à linha preta) do indicador geral (iSegCiber) e dos indicadores relativos a cada um dos controles avaliados (iControle1, iControle2, iControle7, iControle14 e iControle17) (Figura 30). É possível observar que a grande maioria das 377 organizações avaliadas ainda estão nos níveis iniciais de capacidade em gestão de SegCiber ("Inexpressivo": 89; "Inicial": 202).

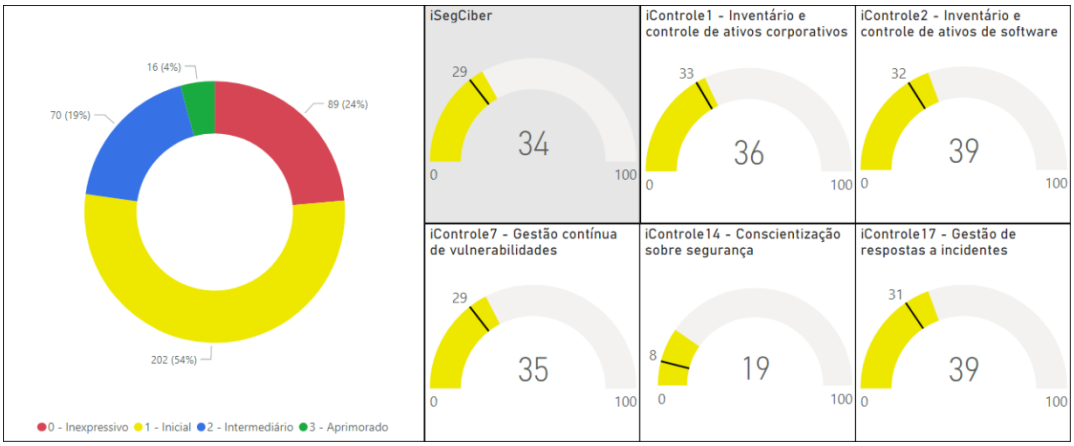
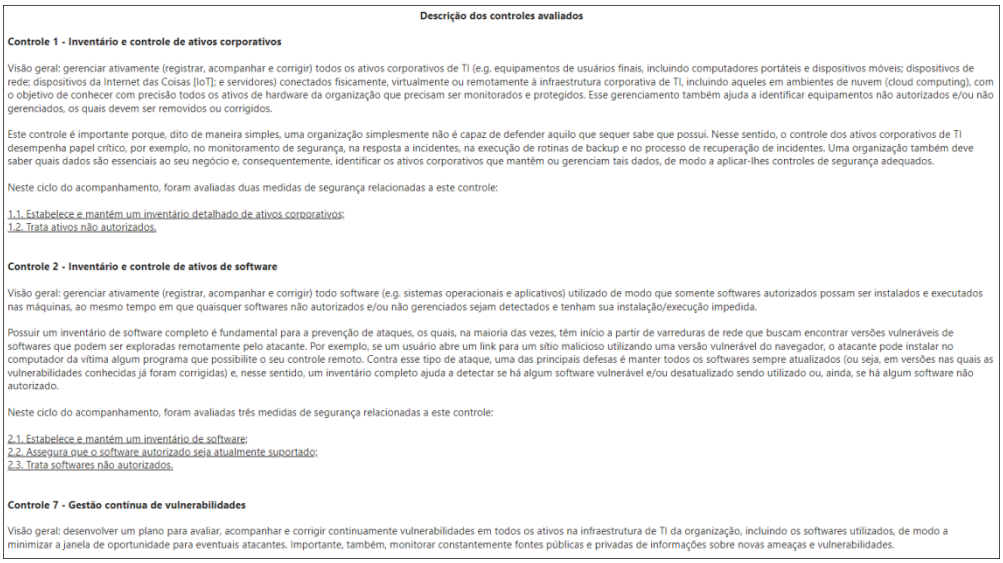



**Figura 30 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Indicadores - resultados".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Controles"

178. Essa aba mostra textos explicativos sobre cada um dos cinco controles avaliados neste ciclo, além de enumerar as respectivas medidas de segurança (Figura 31). Para ver o texto completo, é preciso rolar a tela.



**Descrição dos controles avaliados**

**Controle 1 - Inventário e controle de ativos corporativos**

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todos os ativos corporativos de TI (e.g. equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis; dispositivos de rede; dispositivos da Internet das Coisas [IoT]; e servidores) conectados fisicamente, virtualmente ou remotamente à infraestrutura corporativa de TI, incluindo aqueles em ambientes de nuvem (cloud computing), com o objetivo de conhecer com precisão todos os ativos de hardware da organização que precisam ser monitorados e protegidos. Esse gerenciamento também ajuda a identificar equipamentos não autorizados e/ou não gerenciados, os quais devem ser removidos ou corrigidos.

Este controle é importante porque, dito de maneira simples, uma organização simplesmente não é capaz de defender aquilo que sequer sabe que possui. Nesse sentido, o controle dos ativos corporativos de TI desempenha papel crítico, por exemplo, no monitoramento de segurança, na resposta a incidentes, na execução de rotinas de backup e no processo de recuperação de incidentes. Uma organização também deve saber quais dados são essenciais ao seu negócio e, consequentemente, identificar os ativos corporativos que mantém ou gerenciam tais dados, de modo a aplicar-lhes controles de segurança adequados.

Neste ciclo do acompanhamento, foram avaliadas duas medidas de segurança relacionadas a este controle:

1.1. Estabelece e mantém um inventário detalhado de ativos corporativos;
1.2. Trata ativos não autorizados.

**Controle 2 - Inventário e controle de ativos de software**

Visão geral: gerenciar ativamente (registrar, acompanhar e corrigir) todo software (e.g. sistemas operacionais e aplicativos) utilizado de modo que somente softwares autorizados possam ser instalados e executados nas máquinas, ao mesmo tempo em que quaisquer softwares não autorizados e/ou não gerenciados sejam detectados e tenham sua instalação/execução impedida.

Possuir um inventário de software completo é fundamental para a prevenção de ataques, os quais, na maioria das vezes, têm início a partir de varreduras de rede que buscam encontrar versões vulneráveis de softwares que podem ser exploradas remotamente pelo atacante. Por exemplo, se um usuário abre um link para um sítio malicioso utilizando uma versão vulnerável do navegador, o atacante pode instalar no computador da vítima algum programa que possibilite o seu controle remoto. Contra esse tipo de ataque, uma das principais defesas é manter todos os softwares sempre atualizados (ou seja, em versões nas quais as vulnerabilidades conhecidas já foram corrigidas) e, nesse sentido, um inventário completo ajuda a detectar se há algum software vulnerável e/ou desatualizado sendo utilizado ou, ainda, se há algum software não autorizado.

Neste ciclo do acompanhamento, foram avaliadas três medidas de segurança relacionadas a este controle:

2.1. Estabelece e mantém um inventário de software;
2.2. Assegura que o software autorizado seja atualmente suportado;
2.3. Trata softwares não autorizados.

**Controle 7 - Gestão contínua de vulnerabilidades**

Visão geral: desenvolver um plano para avaliar, acompanhar e corrigir continuamente vulnerabilidades em todos os ativos na infraestrutura de TI da organização, incluindo os softwares utilizados, de modo a minimizar a janela de oportunidade para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

**Figura 31 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Controles".**
(Fonte: painel construído para visualizar as respostas das organizações)

Abas "Controle 1", "Controle 2", "Controle 7", "Controle 14" e "Controle 17"

179. Cada uma dessas abas apresenta, no topo, os gráficos com os valores médios e medianos das avaliações do respectivo indicador (iControle1, iControle2, iControle7, iControle14 e iControle17) e das medidas de segurança correspondentes, os quais foram utilizados para ilustrar as sessões "Situação encontrada" dos riscos identificados neste ciclo do acompanhamento (Figuras 5, 9, 14, 23 e 27).

180. Abaixo desses gráficos, que sintetizam o panorama das organizações avaliadas em relação aos controles críticos de SegCiber e às respectivas medidas de segurança, foram inseridos gráficos contendo as distribuições das respostas das organizações a cada uma das perguntas individuais do

questionário, tanto do "tipo A" quanto do "tipo B". Os gráficos das questões do "tipo A" são mostrados no início das seções correspondentes a cada uma das medidas de segurança (*e.g.* Figura 1), ao passo que os resultados dos gráficos das questões do "tipo B" (Figura 32), para melhor visualização, foram apresentados na forma das tabelas das subpráticas de cada uma dessas medidas (*e.g.* Tabela 2).

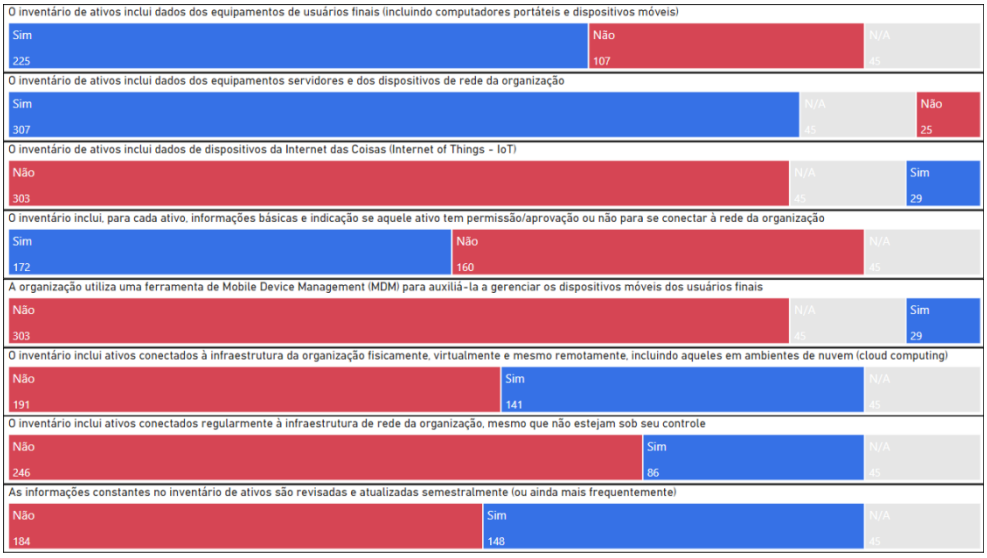
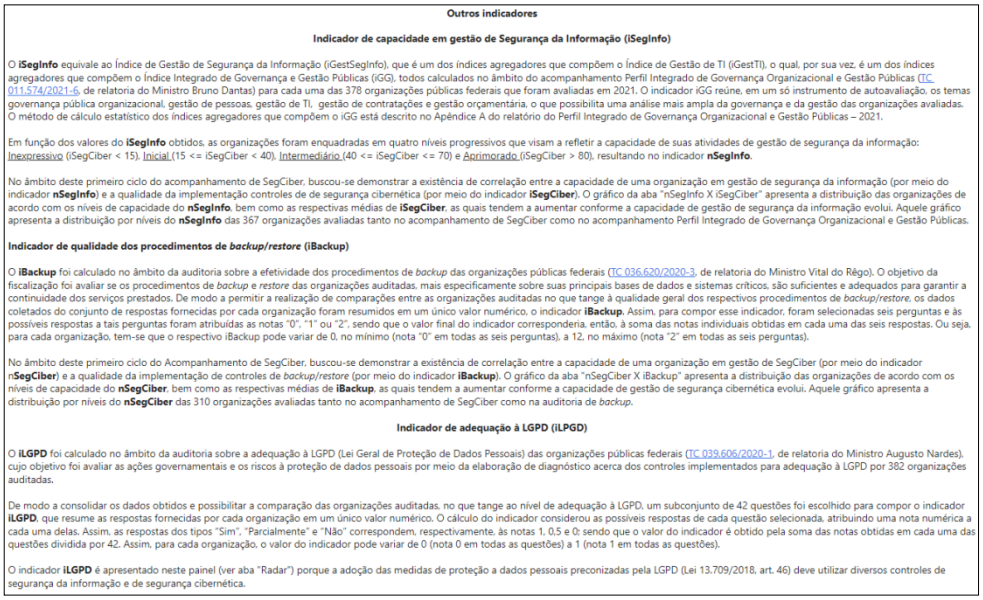



**Figura 32 - Distribuição das respostas à pergunta 1.1.2 do questionário.**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Outros indicadores"

181. Essa aba descreve outros indicadores, relativos a fiscalizações diversas do TCU (iGG, iGestTI, iSegInfo, iBackup, iLGPD), os quais foram utilizados para realizar correlações com os indicadores relacionados aos controles críticos de SegCiber (Figura 33).



**Outros indicadores**

**Indicador de capacidade em gestão de Segurança da Informação (iSegInfo)**

O **iSegInfo** equivale ao Índice de Gestão de Segurança da Informação (iGestSegInfo), que é um dos índices agregadores que compõem o Índice de Gestão de TI (iGestTI), o qual, por sua vez, é um dos índices agregadores que compõem o Índice Integrado de Governança e Gestão Públicas (iGG), todos calculados no âmbito do acompanhamento Perfil Integrado de Governança Organizacional e Gestão Públicas (TC 011.574/2021-6, de relatoria do Ministro Bruno Dantas) para cada uma das 378 organizações públicas federais que foram avaliadas em 2021. O indicador iGG reúne, em um só instrumento de autoavaliação, os temas governança pública organizacional, gestão de pessoas, gestão de TI, gestão de contratações e gestão orçamentária, o que possibilita uma análise mais ampla da governança e da gestão das organizações avaliadas. O método de cálculo estatístico dos índices agregadores que compõem o iGG está descrito no Apêndice A do relatório do Perfil Integrado de Governança Organizacional e Gestão Públicas – 2021.

Em função dos valores do **iSegInfo** obtidos, as organizações foram enquadradas em quatro níveis progressivos que visam a refletir a capacidade de suas atividades de gestão de segurança da informação: Inexpressivo (iSegCiber < 15), Inicial (15 <= iSegCiber < 40), Intermediário (40 <= iSegCiber <= 70) e Aprimorado (iSegCiber > 80), resultando no indicador **nSegInfo**.

No âmbito deste primeiro ciclo do acompanhamento de SegCiber, buscou-se demonstrar a existência de correlação entre a capacidade de uma organização em gestão de segurança da informação (por meio do indicador **nSegInfo**) e a qualidade da implementação controles de segurança cibernética (por meio do indicador **iSegCiber**). O gráfico da aba "nSegInfo X iSegCiber" apresenta a distribuição das organizações de acordo com os níveis de capacidade do **nSegInfo**, bem como as respectivas médias de **iSegCiber**, as quais tendem a aumentar conforme a capacidade de gestão de segurança da informação evolui. Aquele gráfico apresenta a distribuição por níveis do **nSegInfo** das 367 organizações avaliadas tanto no acompanhamento de SegCiber como no acompanhamento Perfil Integrado de Governança Organizacional e Gestão Públicas.

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

O **iBackup** foi calculado no âmbito da auditoria sobre a efetividade dos procedimentos de *backup* das organizações públicas federais (TC 036.620/2020-3, de relatoria do Ministro Vital do Rêgo). O objetivo da fiscalização foi avaliar se os procedimentos de *backup* e *restore* das organizações auditadas, mais especificamente sobre suas principais bases de dados e sistemas críticos, são suficientes e adequados para garantir a continuidade dos serviços prestados. De modo a permitir a realização de comparações entre as organizações auditadas no que tange à qualidade geral dos respectivos procedimentos de *backup/restore*, os dados coletados do conjunto de respostas fornecidas por cada organização foram resumidos em um único valor numérico, o indicador **iBackup**. Assim, para compor esse indicador, foram selecionadas seis perguntas e 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).

No âmbito deste primeiro ciclo do Acompanhamento de SegCiber, buscou-se demonstrar a existência de correlação entre a capacidade de uma organização em gestão de SegCiber (por meio do indicador n**SegCiber**) e a qualidade da implementação de controles de *backup/restore* (por meio do indicador **iBackup**). O gráfico da aba "nSegCiber X iBackup" apresenta a distribuição das organizações de acordo com os níveis de capacidade do **nSegCiber**, bem como as respectivas médias de **iBackup**, as quais tendem a aumentar conforme a capacidade de gestão de segurança cibernética evolui. Aquele gráfico apresenta a distribuição por níveis do **nSegCiber** das 310 organizações avaliadas tanto no acompanhamento de SegCiber como na auditoria de *backup*.

**Indicador de adequação à LGPD (iLPGD)**

O **iLGPD** foi calculado no âmbito da auditoria sobre a adequação à LGPD (Lei Geral de Proteção de Dados Pessoais) das organizações públicas federais (TC 039.606/2020-1, de relatoria do Ministro Augusto Nardes), cujo objetivo foi avaliar as ações governamentais e os riscos à proteção de dados pessoais por meio da elaboração de diagnóstico acerca dos controles implementados para adequação à LGPD por 382 organizações auditadas.

De modo a consolidar os dados obtidos e possibilitar a comparação das organizações auditadas, no que tange ao nível de adequação à LGPD, um subconjunto de 42 questões foi escolhido para compor o indicador **iLGPD**, que resume as respostas fornecidas por cada organização em um único valor numérico. O cálculo do indicador considerou as possíveis respostas de cada questão selecionada, atribuindo uma nota numérica a cada uma delas. Assim, as respostas dos tipos "Sim", "Parcialmente" e "Não" correspondem, respectivamente, às notas 1, 0,5 e 0; sendo que o valor do indicador é obtido pela soma das notas obtidas em cada uma das questões dividida por 42. Assim, para cada organização, o valor do indicador pode variar de 0 (nota 0 em todas as questões) a 1 (nota 1 em todas as questões).

O indicador **iLGPD** é apresentado neste painel (ver aba "Radar") porque a adoção das medidas de proteção a dados pessoais preconizadas pela LGPD (Lei 13.709/2018, art. 46) deve utilizar diversos controles de segurança da informação e de segurança cibernética.

**Figura 33 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Outros indicadores".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba “nSegCiber X iBackup”

182. Essa aba busca mostrar que existe uma correlação positiva entre a capacidade geral de uma organização em gestão de SegCiber (representada pelo indicador nSegCiber) e a respectiva maturidade quanto à implementação de um controle específico (no caso, o controle relativo às rotinas e procedimentos de *backup*/*restore* – TC 036.620/2020-3).

183. O gráfico apresenta a distribuição das organizações de acordo com os respectivos níveis de capacidade em gestão de SegCiber (nSegCiber) e calcula, para cada grupo de organizações, sua nota média no indicador iBackup (ajustada para variar entre 0 e 100). Percebe-se, nitidamente, que essas médias se elevam à medida que as organizações evoluem as suas gestões de SegCiber (Figura 34). Como apenas 310 organizações foram avaliadas em ambas as fiscalizações (acompanhamento de SegCiber e auditoria de *backup*), esse é o somatório dos grupos mostrados (“Inexpressivo”: 76; “Inicial”: 165; “Intermediário”: 57; “Aprimorado”: 12).

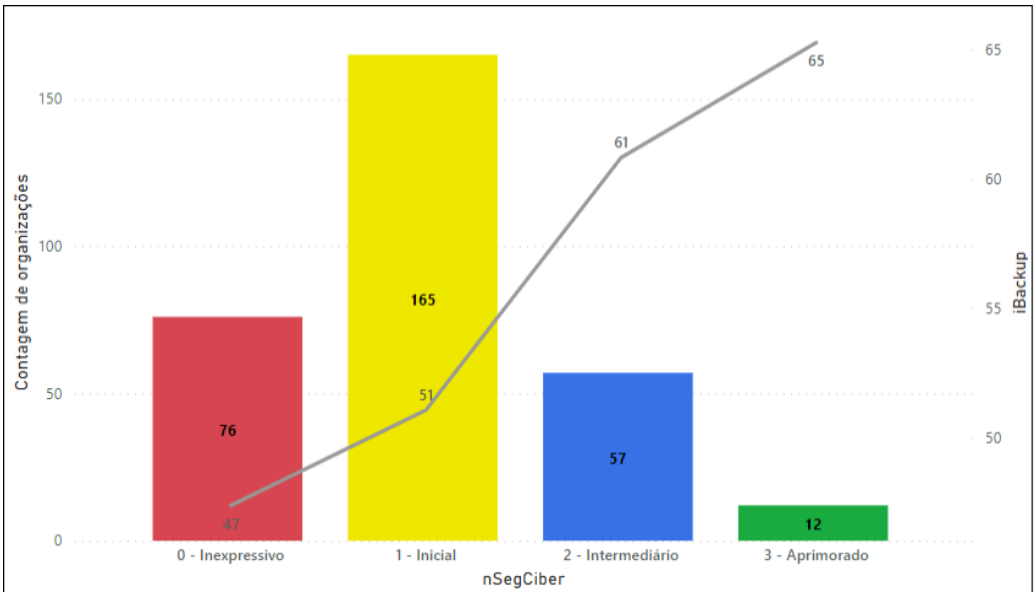



**Figura 34 - Painel “Acompanhamento de controles críticos de SegCiber” - Aba “nSegCiber X iBackup”.**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba “nSegInfo X iSegCiber”

184. Essa aba, a seu turno, procura demonstrar a existência de uma correlação positiva entre a capacidade de uma organização em gestão de SegInfo (refletida pelo indicador nSegInfo) e a respectiva maturidade quanto à implementação de controles críticos de SegCiber (indicador iSegCiber).

185. O modo de obtenção foi parecido. Primeiro, as organizações foram distribuídas de acordo com os respectivos níveis de capacidade em gestão de SegInfo (nSegInfo, derivado do Levantamento Integrado de Governança Organizacional Pública realizado pelo TCU em 2018 [TC 015.268/2018-7]) e, a seguir, foram calculadas, para cada grupo de organizações, sua nota média no indicador iSegCiber. Novamente, é possível perceber que as médias aumentam à medida que as organizações evoluem sua gestão de SegInfo (Figura 35). Nesse caso, como apenas 367 organizações foram avaliadas nessas duas fiscalizações (levantamento de governança e acompanhamento de SegCiber), esse é o somatório dos grupos mostrados (“Inexpressivo”: 74; “Inicial”: 167; “Intermediário”: 94; “Aprimorado”: 32).

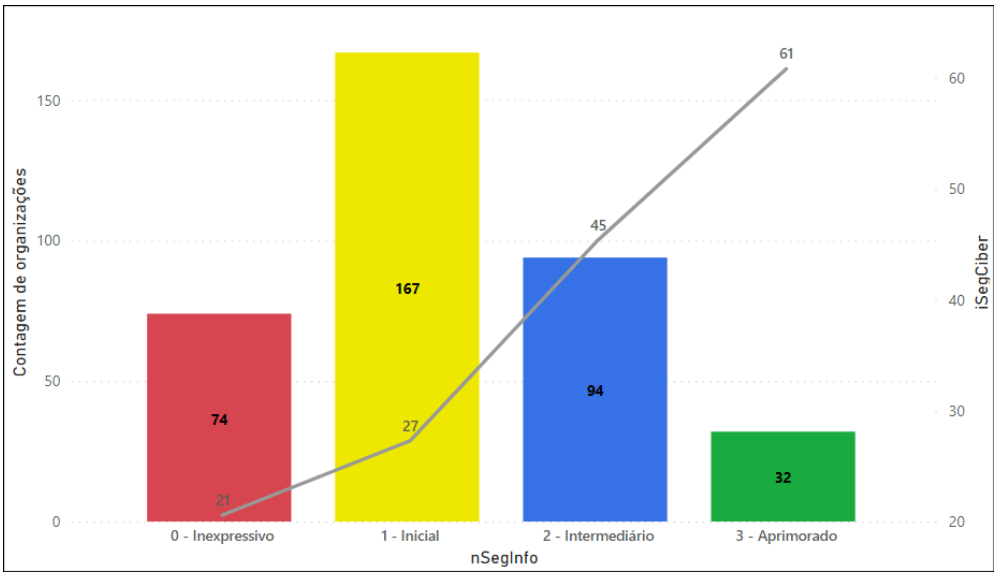



**Figura 35 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "nSegInfo X iSegCiber".**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Radar"

186. Essa aba possui dois gráficos. O da esquerda permite a visualização dos resultados de uma única organização ou, simultaneamente, dos resultados individuais de várias organizações, mostrados de forma sobreposta. O da direita, diferentemente, possibilita a visualização dos resultados de apenas uma organização ou, quando selecionada mais de uma ou mesmo um conjunto amplo de organizações, mostra as médias das notas individuais das organizações que compõem esse grupo (Figura 36).

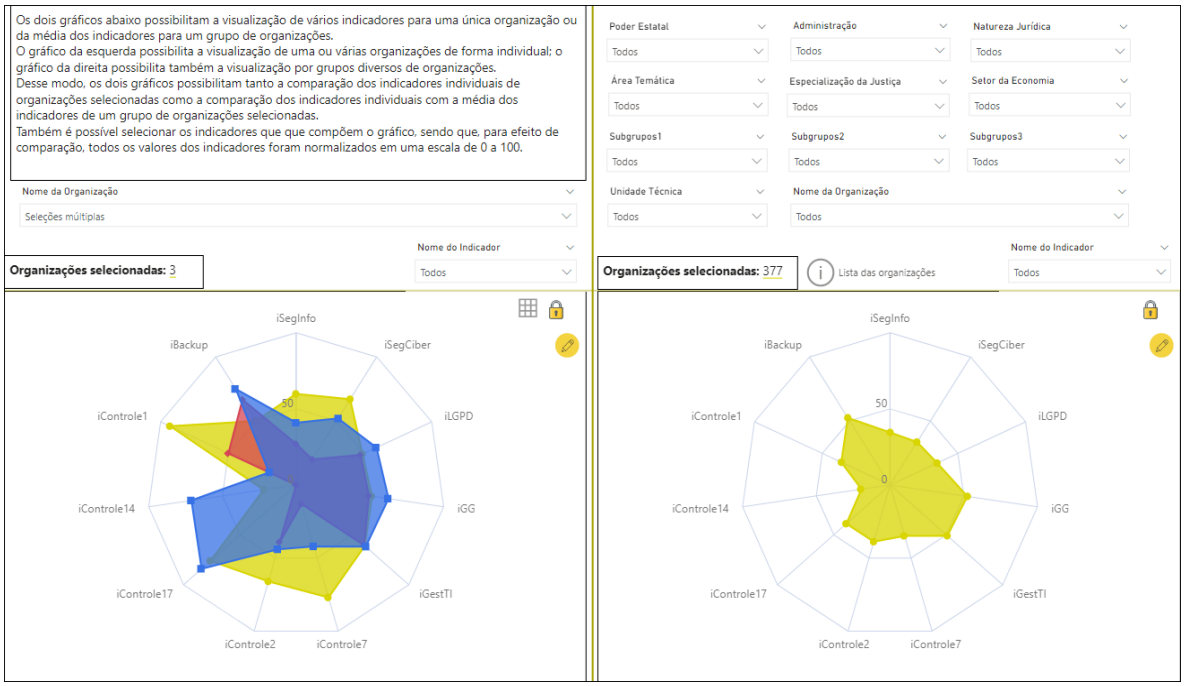



**Figura 36 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Radar".**

(Fonte: painel construído para visualizar as respostas das organizações)

187. Em conjunto, esses gráficos permitem comparar a situação de determinada organização (gráfico à esquerda) com aquela de outra organização específica, do conjunto das 377 organizações participantes do acompanhamento ou mesmo de um subconjunto dessas organizações (gráfico à direita). Em outras palavras, os dois gráficos possibilitam tanto a comparação dos indicadores individuais de organizações selecionadas quanto a comparação desses indicadores individuais com a média dos indicadores de determinado grupo de organizações.

188. Os indicadores que podem ser comparados são aqueles deste acompanhamento (iSegCiber, iControle1, iControle2, iControle7, iControle14 e iControle17 – Figura 30) e de outras fiscalizações do TCU, conforme descritos na aba "Outros indicadores" (iGG, iGestTI, iSegInfo, iBackup, iLGPD), sendo que, para melhorar as comparações, todos os valores foram normalizados para uma escala de 0 a 100. Na Figura 36, por exemplo, nota-se que a organização do gráfico à esquerda apresenta notas superiores às do conjunto das 377 organizações em todos os indicadores, à exceção do iControle1.

189. Para segmentar as comparações, o gráfico à direita permite a aplicação de todos os filtros descritos anteriormente (parágrafo 172 e subparágrafos; Figura 27). Além disso, ambos os gráficos possibilitam restringir os indicadores a serem mostrados na visualização. A característica do gráfico da esquerda de permitir a sobreposição dos resultados de várias organizações acaba sendo efetiva para comparar poucas organizações entre si (Figura 37), caso contrário a figura fica muito "poluída".

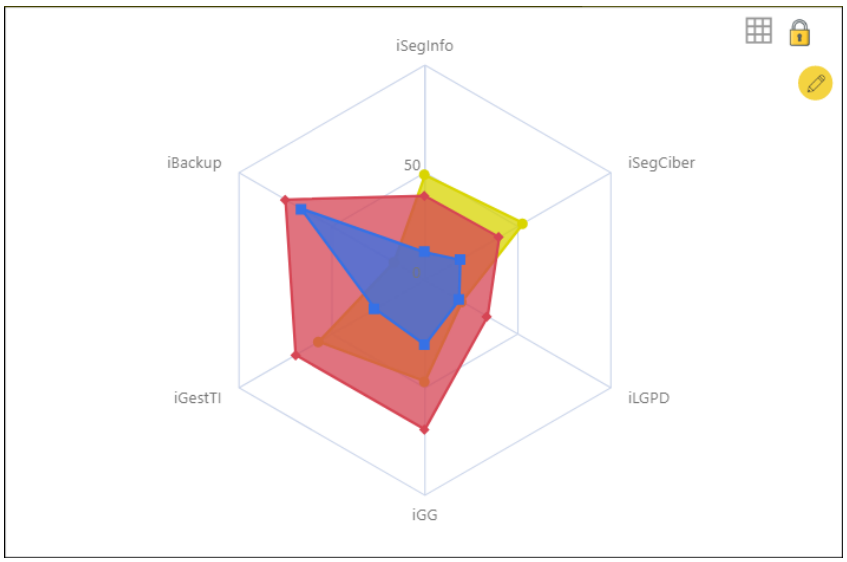



**Figura 37 - Aba "Radar" - Gráfico sobreposto com os resultados de múltiplas organizações.**
(Fonte: painel construído para visualizar as respostas das organizações)

Aba "Lista das organizações"

190. Essa aba apresenta os resultados individuais de todas as 377 organizações que responderam o questionário deste primeiro ciclo do acompanhamento de controles críticos de SegCiber, permitindo, ainda, a seleção de acordo com os filtros já mencionados (parágrafo 172 e subparágrafos; Figura 38).

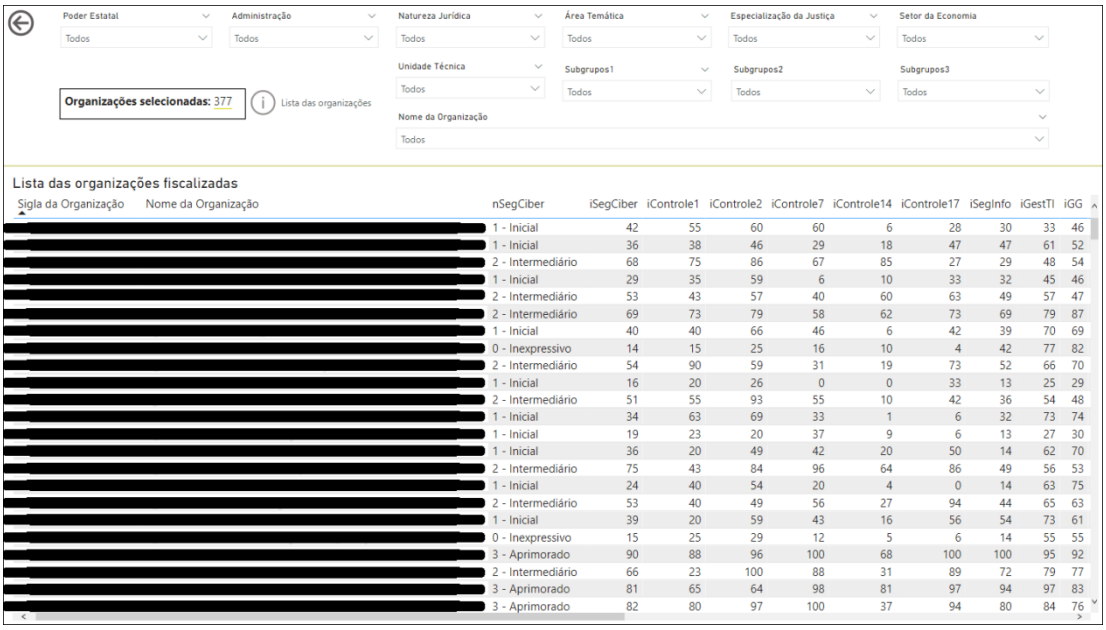



**Figura 38 - Painel "Acompanhamento de controles críticos de SegCiber" - Aba "Lista das organizações".**
(Fonte: painel construído para visualizar as respostas das organizações)

## 5. Propósitos do acompanhamento, relatórios de *feedback* e indicadores de SegCiber

191. 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 levantamento com o objetivo de conhecer a macroestrutura de governança e gestão de SegInfo/SegCiber na APF, incluindo legislação, políticas, normativos, atores, papéis e responsabilidades atinentes a essas áreas. O respectivo relatório sugeriu a "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023"**Error! Bookmark not defined.** (Figura 39) e apontou a necessidade de verificação do nível de preparação das organizações públicas em relação à implantação de controles críticos de SegCiber, além de conscientizá-las para os problemas e os riscos inerentes.

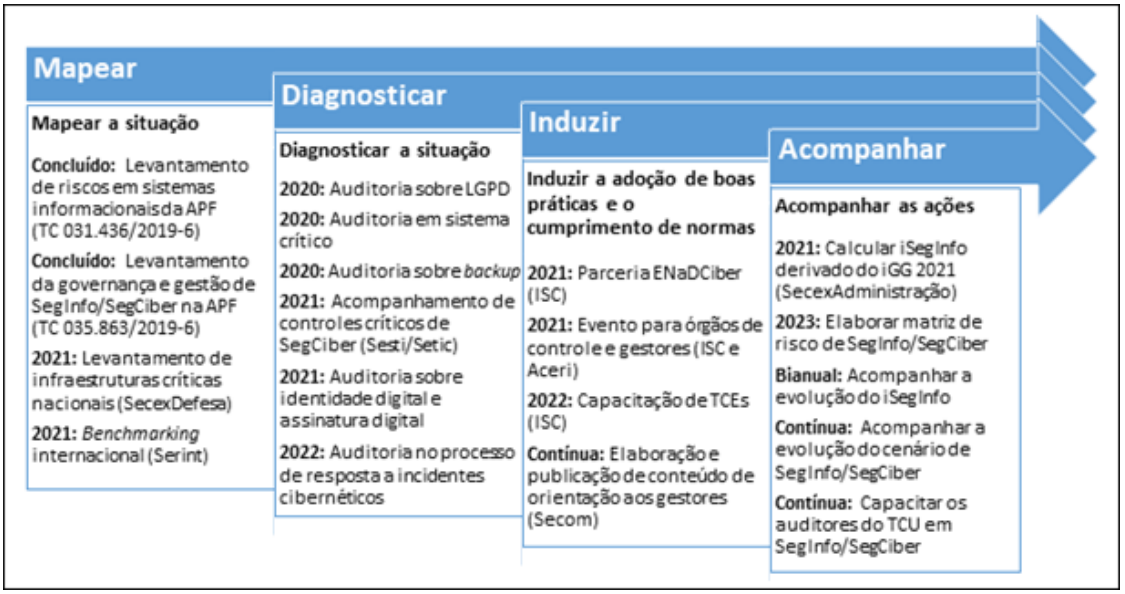



**Figura 39 - Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023.**
(Fonte: TC 001.873/2020-2, peça 46 [relatório], Figura 37)

192. Em seguida, foi realizada uma auditoria-piloto para verificar os controles relativos à execução de procedimentos de *backup* e *restore* (TC 036.620/2020-3; Acórdão 1.109/2021-TCU-Plenário, Rel. Min. Vital do Rêgo), a qual validou a viabilidade da condução desse tipo de fiscalização por meio da aplicação da metodologia CSA. Com isso, foi iniciado este acompanhamento, que visa a obter dados e avaliar a adoção, pelas organizações públicas federais, de controles críticos de SegCiber, conforme previsto na mencionada estratégia (Figura 39).

Propósitos do acompanhamento

193. O propósito geral deste acompanhamento é realizar um mapeamento amplo das organizações públicas federais quanto à implementação de controles críticos de SegCiber, de modo a dotar o TCU de inteligência suficiente para atuar proativamente no sentido de ajudar as organizações a alavancarem tais controles, diminuindo, assim, os riscos relativos ao processo de transformação digital da Administração Pública. Em síntese, esse panorama encontra-se no Capítulo 2, cujas informações poderão ser levadas em consideração na definição de auditorias baseadas em risco (*e.g.* auditar órgãos de maturidade baixa responsáveis por manter sistemas governamentais críticos).

194. Porém, além de gerar esse diagnóstico para o Tribunal, a fiscalização também intencionou conscientizar e orientar os gestores das organizações participantes em relação aos riscos associados à ausência desses controles e das medidas de SegCiber associadas, a exemplo dos ataques cibernéticos, cada vez mais comuns (Capítulo 6), bem como, a partir do cenário percebido (Capítulos 2 e 3), fundamentar propostas de recomendação com vistas a endereçar o aprimoramento desses controles.

195. Com isso, a Sefti espera ajudar as organizações públicas federais a, ao longo dos próximos anos, elevarem suas maturidades em relação a tais controles de SegCiber (tanto os questionados neste ciclo do acompanhamento quanto os que ainda serão avaliados), com reflexos nas respectivas resiliências quanto a falhas de segurança, vulnerabilidades e ataques cibernéticos.

196. Ademais, o acompanhamento poderá municiar os gestores da área de SegInfo, bem como as unidades de auditoria interna dessas organizações, com uma sistemática (CSA – parágrafos 14-15) e ferramentas específicas (*e.g.* questionário [**Error! Reference source not found.**], relatório de *feedback*) para que as próprias organizações continuem se autoavaliando e evoluindo em relação à implementação desses controles.

197. Por fim, o acompanhamento também serviu para fornecer ao Tribunal um painel (*dashboard*) construído para permitir a visualização gráfica e interativa das respostas das organizações, inclusive com a possibilidade de correlação com os resultados de outras fiscalizações e de segmentação das análises a partir da aplicação de filtros diversos.

Relatórios de *feedback* às organizações

198. Na auditoria-piloto (TC 036.620/2020-3, auditoria de *backup*/*restore* dos órgãos e entidades da APF; Rel. Min. Vital do Rêgo)[Error! Bookmark not defined.], de modo a motivar os gestores a aperfeiçoarem os controles envolvidos, foram encaminhados às organizações participantes dois tipos de relatórios de *feedback*, um individual (trazendo comentários e sugestões dos auditores com base nas respostas fornecidas pela própria organização) e outro comparativo (comparando a organização com subgrupos de organizações similares [**Error! Reference source not found.**]). Esses relatórios foram preparados manualmente e, portanto, além de tal tarefa ter consumido diversas horas de trabalho da equipe de auditores, esse *feedback* demorou a chegar aos gestores participantes.

199. De modo a aumentar a efetividade desse retorno, este acompanhamento adotou a automatização da geração do relatório de *feedback* individual na própria ferramenta de aplicação do questionário (LimeSurvey). Assim, ao final do preenchimento, cada gestor participante teve acesso imediato às suas notas nos indicadores relacionados a cada um dos controles verificados (iControle1, iControle2, iControle7, iControle14 e iControle17), bem como à sua avaliação geral de maturidade

(iSegCiber) e ao nível de SegCiber correspondente (Inexpressivo, Inicial, Intermediário ou Aprimorado).

200. Adicionalmente, para os subgrupos de organizações definidos (**Error! Reference source not found.**), serão elaborados relatórios de *feedback* comparativos utilizando gráficos obtidos a partir do painel descrito no Capítulo 4, de modo que cada gestor possa comparar os resultados individuais da sua organização com a realidade de um grupo de organizações similares a ela e, assim, ter mais incentivos para continuar evoluindo, ao longo dos próximos meses e anos, em relação à implementação dos controles e medidas de segurança verificados.

Indicadores de SegCiber

201. De modo a permitir a comparação entre as 377 organizações participantes no que tange aos níveis de maturidade em relação a cada um dos controles verificados neste ciclo do acompanhamento, tomados individualmente, foram criados, a partir das respostas fornecidas no questionário, os indicadores iControle1, iControle2, iControle7, iControle14 e iControle17. Também foi criado um indicador para, com base nesse conjunto de controles, sintetizar a maturidade geral da organização em SegCiber (iSegCiber). A sistemática de cálculo desses indicadores é explicada a seguir.

202. Para cada uma das medidas de segurança avaliadas, o questionário trazia duas perguntas: uma primeira do "tipo A" (questionando o grau de adoção daquela medida na organização) e uma segunda do "tipo B" (solicitando a marcação das subpráticas específicas, relativas àquela medida de segurança, que se encontram efetivamente implementadas na organização).

203. Na questão do "tipo A", de acordo com o grau de adoção da medida na organização, foi atribuída a seguinte nota: 0 (zero), se a medida não é adotada ou foi considerada não aplicável; 10 (dez), se apenas há decisão formal ou plano aprovado para adotá-la; 25 (vinte e cinco), se a medida é adotada em menor parte; 50 (cinquenta), se a medida é adotada parcialmente; e 100 (cem), se a medida é adotada em maior parte ou totalmente. Na questão do "tipo B", a nota foi atribuída (entre 0 e 100) na proporção das subpráticas marcadas pelo gestor como implementadas (por exemplo, se havia duas subpráticas e o gestor marcou apenas uma delas, a nota atribuída foi 50 [cinquenta]; se havia três subpráticas e o gestor marcou duas delas, a nota atribuída foi 66 [sessenta e seis]). A nota final atribuída a cada medida de segurança, então, correspondeu à média ponderada das notas dessas duas questões (questão do tipo A: peso 60; questão do tipo B: peso 40).

204. Em seguida, os valores dos indicadores atribuídos a cada um dos controles (iControle1, iControle2, iControle7, iControle14 e iControle17) corresponderam à média simples das notas obtidas nas respectivas medidas de segurança e o valor do indicador geral (iSegCiber), a seu turno, foi a média simples dos valores obtidos nos cinco controles (iControle1 + iControle2 + iControle7 + iControle14 + iControle17 / 5). Assim, todos os valores das notas de questões individuais ("tipo A" ou "tipo B"), das notas de medidas de segurança individuais e dos indicadores criados (iControle1, iControle2, iControle7, iControle14, iControle17 e iSegCiber) variam entre 0 e 100.

205. Por fim, em função dos valores do iSegCiber, cada organização foi enquadrada em um de quatro níveis progressivos (nSegCiber) para refletir a maturidade das suas atividades de SegCiber (Tabela 22). O gráfico da Figura 30 apresenta o quantitativo da distribuição das 377 organizações avaliadas nesses quatro níveis de maturidade em SegCiber.

**Tabela 22 - Níveis progressivos de maturidade em SegCiber das organizações (nSegCiber).**
(Fonte: elaboração própria)

| iSegCiber | nSegCiber |
|---|---|
| iSegCiber <= 15 | Inexpressivo |
| 15 < iSegCiber <= 50 | Inicial |
| 50 < iSegCiber <= 80 | Intermediário |
| iSegCiber > 80 | Aprimorado |

206. Esses níveis de maturidade permitem também comparação com resultados de outros trabalhos de avaliação já realizados pelo TCU em áreas conexas. Neste acompanhamento, por exemplo, procurou-se demonstrar a existência de uma correlação positiva entre a capacidade de uma organização em gestão de SegInfo (avaliada no acompanhamento do Perfil Integrado de Governança Organizacional e Gestão Públicas 2021 [parágrafos 247-256]), de modo geral, e a implementação, na prática, de controles específicos de SegCiber (no caso deste ciclo, dos cinco controles avaliados [parágrafos 7.1-7.5]). Em outras palavras, buscou-se mostrar que, efetivamente, as organizações com maior maturidade em gestão de SegInfo adotam boas práticas quando se trata de controles de SegCiber, isto é, tendem a implementar as medidas de segurança avaliadas neste acompanhamento (Figura 35).

207. Entretanto, ressalva-se que as faixas adotadas no âmbito do acompanhamento do Perfil Integrado de Governança Organizacional e Gestão Públicas 2021 (indicadores iGG, iGestTI e iSegInfo) são diferentes: Inexpressivo: 0 a 14,99%, Iniciando: 15 a 39,99%, Intermediário: 40 a 70% e Aprimorado: 70,01 a 100% (TC 011.574/2021-6, peça 1.060 [relatório consolidador], Figura 4).

## 6. Cenário atual de SegCiber

208. Este capítulo busca contextualizar o cenário atual de SegCiber no mundo e no Brasil, com vistas a transmitir, de maneira mais objetiva, o tamanho atual do problema e a sua tendência ao longo dos últimos anos.

209. O processo de transformação digital dos serviços públicos traz facilidades, com cada vez mais informações e sistemas relevantes e críticos disponíveis na Internet. Porém, com isso, também aumentam bastante os riscos decorrentes de ameaças e ataques cibernéticos, uma vez que vulnerabilidades e falhas de SegInfo, então, passam a afetar significativamente o governo e os cidadãos.

210. Além disso, o acesso à Internet e o trabalho remoto aumentaram consideravelmente devido à pandemia da Covid-19, levando criminosos cibernéticos a aumentarem a disseminação (por meio de ataques de *phishing*, por exemplo) de *malwares* com vistas a capturar informações pessoais ou exigir o resgate de arquivos criptografados (ataques de *ransomware*[xvii]). Para se ter ideia do risco ao qual as organizações estão expostas, basta constatar que, segundo dados da Kaspersky, em 2020 o Brasil era "alvo de quase metade dos ataques de *ransomware* na América Latina"[xviii] e as empresas brasileiras eram as que mais sofriam esse tipo de ataque no mundo[xix], com tendência de aumento do problema para 2021[xx].

211. De acordo com informações da empresa Fortinet, que coleta e analisa diariamente incidentes de SegCiber em todo o mundo, em 2020 haviam ocorrido mais de 41 bilhões de tentativas de ataques cibernéticos na América Latina (das quais 8,4 bilhões no Brasil)[xxi], número que, somente na primeira metade de 2021, subiu para mais de 91 bilhões na América Latina (16,2 bilhões no Brasil)[xxii].

212. Em âmbito global, a Fortinet frisou que a quantidade de ataques de *ransomware* continua aumentando devido à crescente utilização do modelo chamado *Ransomware-as-a-Service* (RaaS), no qual os criminosos se concentram na obtenção e na venda do acesso inicial às redes a serem atacadas. A empresa mostrou que as campanhas de *phishing* ainda são o principal vetor de ataque e apontou, também, o aumento na atividade de *botnets* tendo como alvos dispositivos IoT, a grande onda de tentativas de exploração de vulnerabilidades e o modo como a intensificação do trabalho remoto acabou atuando como porta de entrada para as redes corporativas. Com relação a novas tecnologias, destacou o uso da inteligência artificial, que está aumentando as chances de sucesso dos criminosos, bem como a chegada da conectividade 5G, que possibilitará novas ameaças em velocidade e escala sem precedentes.

213. Como forma de proteção, além das defesas técnicas, a empresa ressaltou que o treinamento e a conscientização contínuos sobre SegCiber são fundamentais para que os funcionários

da organização atuem como a primeira barreira contra ataques de engenharia social, *phishing*, *malware* e outros.

214. A seu turno, a Kaspersky, outra empresa do mercado de SegCiber, destacou que, durante a pandemia, o Brasil foi o país mais afetado por ataques de *ransomware* direcionados a empresas, num contexto em que o crime cibernético aproveitou a mudança de muitos funcionários para o regime de trabalho remoto (*home office*) para intensificar a disseminação de ameaças pela Internet. Dentre outras medidas de segurança, a empresa também destacou as atualizações imediatas e frequentes dos softwares utilizados e os treinamentos de conscientização em SegCiber para capacitar os funcionários a identificarem os riscos e trabalharem com mais segurança, em casa ou no escritório[xxiii].

215. No levantamento "Panorama de Ameaças 2021", a Kaspersky mostrou que os ataques cibernéticos no Brasil aumentaram 23% nos oito primeiros meses de 2021, em comparação com o mesmo período do ano anterior. De acordo com os analistas da empresa, a segurança do trabalho remoto precisa ser levada a sério e a pirataria deve ser eliminada das casas e dos ambientes empresariais[xxiv]. A Kaspersky apontou, ainda, a tendência de aumento nos ataques direcionados a serviços na nuvem: "enquanto para as empresas a nuvem significa flexibilidade e economia, para os *hackers* é um ambiente repleto de dados corporativos, *apps* e outros ativos *online* com proteção ruim"[xxv].

216. Na mesma linha, o relatório anual 2021 do *National Cyber Security Centre* (NCSC) do Reino Unido apontou que as ameaças cibernéticas continuam crescendo: de golpes de *phishing* em massa contra vítimas indiscriminadas, passando por ataques de *ransomware* contra organizações públicas e privadas e chegando até atos hostis direcionados contra infraestruturas críticas de governo[xxvi]. De acordo com esse centro, o impacto real desses ataques naquele país e em todo o mundo foi gritante: economias pessoais foram roubadas, o suprimento de alimentos e o fornecimento de energia foram afetados, os preços dos combustíveis locais aumentaram, os cidadãos foram impedidos de acessar serviços públicos e dados críticos e confidenciais foram comprometidos.

217. O NCSC também destacou a exploração da Covid-19 como oportunidade pelos criminosos cibernéticos, no sentido de que a pandemia acelerou a digitalização de empresas e governos locais, aumentando a oferta de serviços *online* e a confiança na utilização da computação em nuvem, o que ampliou a superfície de ataque e tornou a SegCiber mais desafiadora para as organizações. Além disso, estados hostis direcionaram suas operações cibernéticas para roubar vacinas e pesquisas médicas.

218. Ademais, o NCSC destacou os ataques sofisticados a elementos menos seguros na cadeia de suprimentos (*supply chain*) de instituições econômicas, governamentais e de segurança nacional, observando a gravidade dos ataques contra a plataforma de gerenciamento de TI SolarWinds[xxvii] e os servidores Microsoft Exchange[xxviii]. O centro considerou o *ransomware* como a mais significativa ameaça cibernética enfrentada pelo Reino Unido em 2021 e destacou o modelo RaaS, no qual credenciais *online* e variantes de *malware* prontas para uso são disponibilizadas para os criminosos mediante pagamento ou participação nos lucros.

219. Para 2022, a empresa de segurança Netskope previu alguns pontos de preocupação imediata (aumento dos ataques voltados a APIs e das ameaças e vulnerabilidades causadas por funcionários, pelo avanço da IA/*machine learning*, pelo retorno ao regime de trabalho presencial e pela necessidade de acesso remoto [*e.g.* VPNs, *endpoints*]) e outros de mais longo prazo (crescimento dos ataques de *ransomware*, *phishing* e abuso das autorizações de acesso por aplicativos, neutralização da "pegada de carbono" dos *data centers*, aumento de *malwares* em documentos do Office, surgimento do conceito *Security Service Edge* [SSE] e explosão dos casos de desinformação, clonagem de voz e *deepfakes*)[xxix].

220. Os analistas da companhia *Enterprise Strategy Group* (ESG), a seu turno, preveem cinco grandes tendências de SegCiber para 2022: aumento da segurança de ambientes domésticos por meio da implementação de soluções de *Secure Access Service Edge* (SASE), maior preocupação com a segurança de APIs, consolidação das soluções de *Extended Detection and Response* (XDR), crescimento dos casos de ataque interno (por colaboradores da própria organização) e ascensão das plataformas denominadas *Security Observability, Prioritization and Validation* (SOP-V)[xxx].

Cenário de incidentes na APF

221. Relativamente à APF, de acordo com o Anexo I do Decreto 9.668/2019[xxxi], compete ao GSI/PR "planejar, coordenar e supervisionar a atividade de [SegInfo] (...), nela incluídos a [SegCiber], a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas" (art. 1º, inciso V). Dentro da estrutura do GSI, essa competência é exercida pelo Departamento de Segurança da Informação (DSI), responsável por elaborar normativos e requisitos metodológicos, bem como por manter o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) e, por meio dele, coordenar a rede de ETIRs formada por órgãos e entidades públicos (art. 16-A, incisos III-VI, incluído pelo Decreto 10.363/2020[xxxii]).

222. No mesmo sentido, o recente Decreto 10.748/2021[xvi] instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (REGIC), com a participação obrigatória dos órgãos e entidades da APF direta, autárquica e fundacional e voluntária por parte das empresas públicas e sociedades de economia mista federais, bem como de suas subsidiárias (art. 1º, §§ 1º e 2º), sob a coordenação do DSI, ao qual compete, por meio do CTIR Gov, dentre outras atribuições (arts. 5º, § 1º, e 11):

> I - coordenar as atividades das [ETIRs] dos integrantes da [REGIC] relativas à prevenção, ao tratamento e à resposta aos incidentes cibernéticos;
> VI - difundir alertas, recomendações e estatísticas sobre incidentes cibernéticos para os integrantes da [REGIC]; e
> VII - manter atualizado o sítio eletrônico do [CTIR Gov] com alertas, recomendações e estatísticas sobre incidentes cibernéticos (...).

223. O CTIR Gov, então, recebe notificações das ETIRs dos integrantes da REGIC, o que lhe permite atuar como ponto central de coordenação das ações de resposta a incidentes, coletando informações que podem ser utilizadas, também, para determinar tendências e padrões de atividades de ataques e para recomendar estratégias de prevenção adequadas para toda a APF. Seu sítio disponibiliza o painel "CTIR Gov Em Números", contendo as "estatísticas resultantes do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos"[xxxiii] (Figura 40).

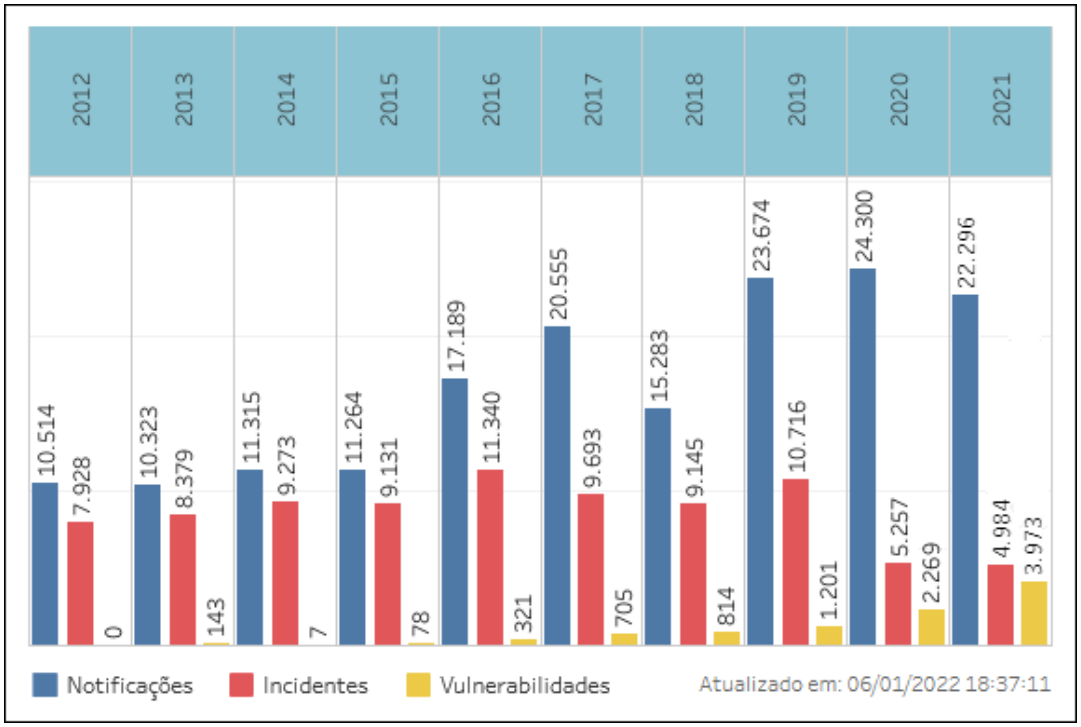



**Figura 40 - Notificações reportadas e incidentes/vulnerabilidades confirmados pelo CTIR Gov.**

- Notificações: todos os eventos detectados e/ou reportados ao CTIR Gov pelo e-mail "ctir@ctir.gov.br";
- Incidentes: notificações que, após triagem, são caracterizadas como evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
- Vulnerabilidades: notificações que, após triagem, são caracterizadas como fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

(Fonte: Painel "CTIR Gov Em Números"[xxxiii])

224. Esses dados mostram que, ao longo dos últimos três anos, o número de notificações reportadas ao CTIR Gov tem se mantido em patamares superiores a 22.000 por ano. Em 2019, quase metade das notificações foram confirmadas como incidentes. Porém, em 2020 e 2021, as confirmações não atingiram um quarto do número de notificações (Figura 40).

225. A Tabela 23 apresenta as quantidades de incidentes e vulnerabilidades confirmadas por categoria, bem como as respectivas variações percentuais de 2020 para 2021. Para 2018 e 2019, os números derivam da base de dados obtida do CTIR Gov no âmbito do levantamento da governança e gestão de SegInfo/SegCiber da APF (TC 001.873/2020-2, relatório, Tabela 5), levando a totais (9.146, 814, 10.828 e 1.192) levemente divergentes daqueles informados na Figura 40 (9.145, 814, 10.716 e 1.201, respectivamente). Em relação às vulnerabilidades de 2020 e 2021, percebe-se que os números mostrados na Figura 40 (2.269 e 3.973) não consideram aquelas categorizadas como "Outras".

**Tabela 23 - Incidentes confirmados por categoria (2018 a 2021).**
(Fonte: 2018 e 2019: TC 001.873/2020-2, relatório, Tabela 5; 2020 e 2021: peça 804, p. 3)

| Categoria do incidente/vulnerabilidade | 2018 | 2019 | 2020 | 2021 | Variação (%) |
|---|---|---|---|---|---|
| Abuso de sítio | 1.940 | 2.978 | 2.525 | 2.015 | -20,2 |
| Fraude | 2.651 | 2.200 | 1.410 | 1.041 | -26,2 |
| *Scan** | 702 | 1.306 | 578 | 595 | +2,9 |
| *Malware*** | 446 | 352 | 75 | 388 | +417,3 |
| Vazamento de informação | 1.793 | 2.421 | 343 | 196 | -42,9 |
| Indisponibilidade | 1.252 | 1.216 | 103 | 5 | -95,2 |
| Outros incidentes | 362 | 355 | 223 | 744 | +233,6 |
| **Subtotal (incidentes)** | **9.146** | **10.828** | **5.257** | **4.984** | **-5,2** |
| Vulnerabilidade DDoS*** | 807 | 1.175 | 1.281 | 1.728 | +34,9 |
| Vulnerabilidade SSL/TLS**** | 7 | 10 | 988 | 2.245 | +127,2 |
| Outras vulnerabilidades | 0 | 7 | 223 | 2 | -99,1 |
| **Subtotal (vulnerabilidades)** | **814** | **1.192** | **2.492** | **3.975** | **+59,5** |
| **TOTAL** | **9.960** | **12.020** | **7.749** | **8.959** | **+15,6** |

*Varredura de rede para mapear computadores ativos e serviços neles disponíveis.
**Software malicioso, do inglês *malicious software*.
*** Negação de Serviço (Distribuída) / (*Distributed*) *Denial of Service*
**** *Secure Socket Layer*/*Transport Layer Security*

226. Percebe-se que, de 2019 para 2020, houve redução superior a 50% no total de incidentes confirmados pelo CTIR Gov, patamar que se manteve em 2021. Para algumas categorias, como

"Vazamento de informação" e "Indisponibilidade", as reduções (de 2019 para 2020) superaram 90%. Questionado a respeito, o CTIR Gov disse que, a partir de 2020, passou a "atuar não somente no tratamento dos incidentes cibernéticos, mas na [sua] prevenção" e que "um dos [seus] processos de melhoria contínua (...), é o ajuste de critérios em caracterizar os incidentes". Sobre a alta no número de vulnerabilidades confirmadas (Figura 40: 2018: 814; 2019: 1.201; 2020: 2.269; 2021: 3.973), afirmou tratar-se de "reflexo de um fenômeno global, conforme notificações de fabricantes e desenvolvedores como também por instituições voltadas para atividade de cibersegurança" (peça 804, p. 2).

227. A seu turno, a Tabela 24 detalha os incidentes da categoria "Abuso de sítio" (desfiguração do conteúdo de páginas da Internet ou comprometimento da segurança de servidores *web*). Percebe-se que, de 2020 para 2021, houve redução geral de 20,2% desse tipo de incidente, sendo que os casos de "Exposição de código" (o atacante obtém conteúdo de código fonte de programas ou de arquivos de configuração de servidores na Internet) e "Listagem de diretório" (o atacante consegue listar diretórios em servidores na Internet, facilitando a descoberta de arquivos com informações sensíveis) praticamente cessaram (reduções de 93,2% e 97,8%, respectivamente). Os casos de "Abuso de fórum/comentários", "Conteúdo incompatível" e "Redirecionamento de página" também tiveram reduções significativas (86,7%, 86,4% e 74,1%, respectivamente).

228. Os casos de "*Spamdexing*"[xxxiv] (o atacante manipula um mecanismo de busca para aumentar artificialmente a relevância de um site), contudo, triplicaram de 2018 para 2019, continuaram subindo de 2019 para 2020 e aumentaram 140,4% de 2020 para 2021, tornando-se, junto com a "Desfiguração de sítio" (o atacante altera conteúdo de páginas na Internet), os incidentes mais comuns. Os valores totais (2018: 1.940; 2019: 2.978; 2020: 2.525; 2021: 2.015), naturalmente, são os mesmos da Tabela 23.

**Tabela 24 - Incidentes da categoria "Abuso de sítio" (2018 a 2021).**
(Fonte: 2018 e 2019: TC 001.873/2020-2, relatório, Tabela 6; 2020 e 2021: peça 804, p. 3)

| Tipo de "Abuso de sítio" | 2018 | 2019 | 2020 | 2021 | Variação (%) |
|---|---|---|---|---|---|
| Desfiguração de sítio | 1.568 | 1.392 | 1.177 | 1.234 | +4,8 |
| Exposição de código | 75 | 576 | 339 | 23 | -93,2 |
| Listagem de diretório | 127 | 505 | 276 | 6 | -97,8 |
| *Spamdexing* | 54 | 159 | 225 | 541 | +140,4 |
| Possível vulnerabilidade | 57 | 148 | 121 | 147 | +21,5 |
| Abuso de fórum/comentários | 14 | 120 | 285 | 38 | -86,7 |
| Conteúdo incompatível | 6 | 29 | 66 | 9 | -86,4 |
| Redirecionamento de página | 21 | 19 | 27 | 7 | -74,1 |
| *Cross Site Scripting* (XSS) | 18 | 17 | 8 | 10 | +25 |
| Mineração de criptomoeda | 0 | 1 | 1 | 0 | -100 |
| Outros | 0 | 12 | - | - | - |
| **Total** | **1.940** | **2.978** | **2.525** | **2.015** | **-20,2** |

229. Diante desse cenário, destacam-se, em 2021, os alertas emitidos pelo CTIR Gov sobre vulnerabilidades em sistemas de autenticação de usuários[xxxv], ações maliciosas em ambientes de nuvem[xxxvi] e ataques de *ransomware* diversos, incluindo RaaS[xxxvii]. O CTIR Gov apontou, também, tendências de ameaças cibernéticas às infraestruturas críticas e aos sistemas de informação da APF, de modo que a "segurança por obscuridade" não deve ser a única medida de segurança[xxxviii].

Cenário de incidentes no Brasil

230. Outra entidade que mantém estatísticas sobre notificações de incidentes a ele reportados de forma voluntária é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), grupo de resposta a incidentes de segurança (*Computer Security Incident Response Team* – CSIRT) de responsabilidade nacional[xxxix] que trata incidentes em computadores conectados à Internet no Brasil. Seu público-alvo engloba organizações que possuam: i) domínios com final ".br"; ii) endereços IP alocados no Brasil; iii) Sistemas Autônomos alocados no Brasil. Nota-se que, em 2014 (ano em que o Brasil sediou a Copa do Mundo de Futebol), foram reportados mais de um milhão de incidentes e, a partir de 2015, aproximadamente 700.000 incidentes/ano, com leves picos em 2017 e 2019 (Figura 41)[xl].

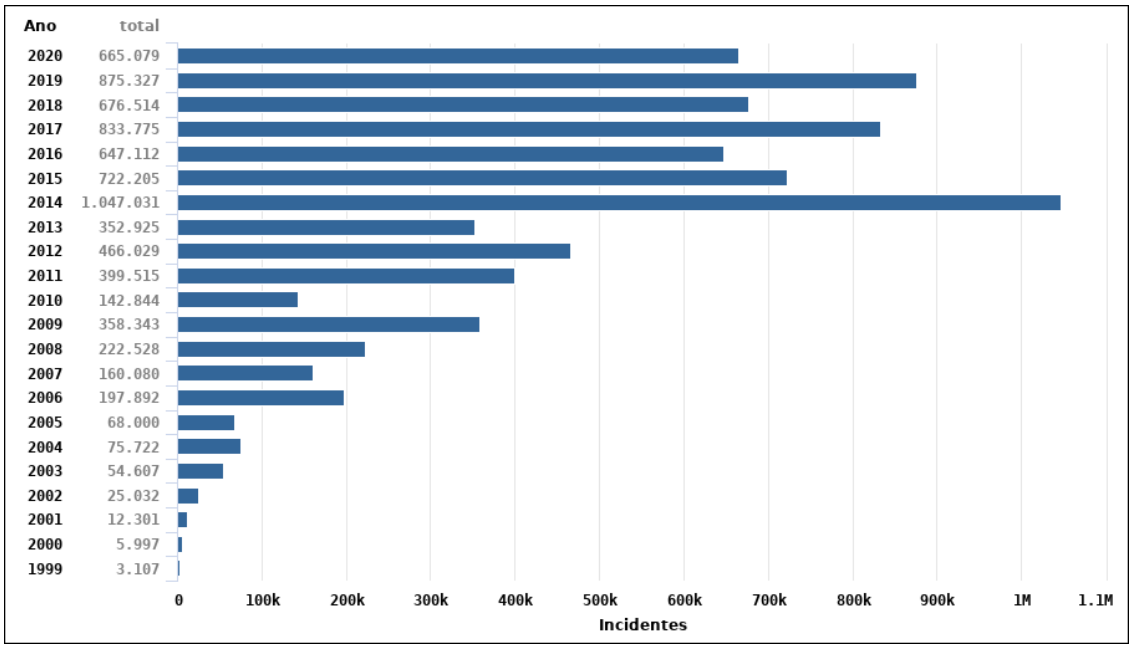



**Figura 41 - Total de incidentes reportados ao CERT.br por ano.**
(Fonte: https://www.cert.br/stats/incidentes)

231. A Figura 42 apresenta a distribuição dos incidentes reportados ao CERT.br, por tipo de ataque, no ano de 2020. Diferentemente do perfil dos incidentes tratados pelo CTIR Gov (Tabela 23), percebe-se que os ataques mais prevalentes foram do tipo "*Scan*" (59,85%), varredura da rede para mapear os computadores ativos e os serviços neles disponíveis (primeiro passo dos atacantes para identificar potenciais alvos vulneráveis), "*Worm*" (20,15%), relacionados à propagação automatizada de códigos maliciosos na rede, e "DoS" (10,25%), acrônimo para "negação de serviço" (*Denial of Service*), no qual o atacante utiliza um computador ou um conjunto de computadores/dispositivos para tirar de operação ("derrubar") um serviço, um computador ou, até mesmo, uma rede inteira.

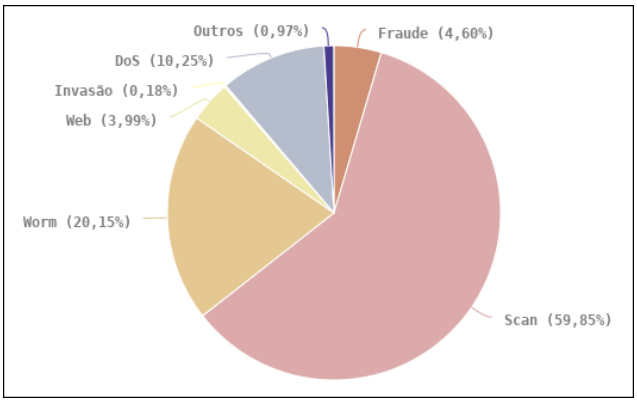



**Figura 42 - Distribuição dos incidentes reportados ao CERT.br por tipo de ataque (2020).**
(Fonte: https://www.cert.br/stats/incidentes/2020-jan-dec/tipos-ataque.html)

232. O sítio da instituição traz, também, uma seção chamada "Análise de alguns fatos de interesse [no período de janeiro a dezembro de 2020]", a qual registra que "o total de notificações recebidas pelo CERT.br em 2020 foi de 665.079", número 24% menor do que em 2019 (Figura 41). A seguir, são mostradas estatísticas e avaliações específicas sobre as diversas categorias de incidentes: "Tentativas de Fraude", "Ataques de Negação de Serviço", "Varreduras e propagação de códigos maliciosos", "Ataques a servidores Web", "Computadores comprometidos" e "Outros incidentes reportados"[xli].

233. Dentre os comentários sobre "Ataques a servidores Web", por exemplo, destaca-se que esses "totalizaram 26.567 em 2020", aumento de 19% em relação a 2019, e que "os ataques incluídos nesta categoria são as buscas por vulnerabilidades em aplicações Web para tentar comprometer estes sistemas e então realizar as mais diversas ações, tais como: hospedar páginas falsas de instituições financeiras, armazenar ferramentas utilizadas em ataques, realizar desfigurações e propagar spam e/ou scam".

Incidente no Ministério da Saúde

234. Recentes incidentes cibernéticos ocorridos em dezembro de 2021 em aproximadamente 23 organizações públicas federais, especialmente no Ministério da Saúde (MS), ilustram de forma concreta a importância da gestão de SegCiber e os impactos decorrentes de falhas e vulnerabilidades em sítios e sistemas críticos de governo.

235. Em 10/12/2021, o MS emitiu nota oficial informando sobre um incidente que comprometeu e deixou indisponíveis alguns de seus sistemas e serviços digitais, tais como o e-SUS Notifica, o Sistema de Informação do Programa Nacional de Imunização (SI-PNI) e o ConecteSUS, bem como as emissões do Certificado Nacional de Vacinação Covid-19 e da Carteira Nacional de Vacinação Digital[xlii].

236. No mesmo dia, a Polícia Federal (PF) publicou nota à imprensa sobre sua atuação no ataque *hacker* ao MS, informando ter sido acionada "para atender ocorrência de ataque cibernético aos sistemas do [MS] e de modificação do conteúdo exibido em seu site (defacement)" e que o incidente teria sido "no ambiente de nuvem pública (AWS), com comprometimento de sistemas de notificação de casos de Covid, do Programa Nacional de Imunização e do Conect[e]SUS"[xliii].

237. Ainda segundo a PF, as primeiras análises periciais para a investigação policial constataram "que os bancos de dados de sistemas do [MS] não foram criptografados pelos hackers", o que, em tese, descartaria a possibilidade de um ataque de *ransomware*, conforme havia noticiado, inicialmente, o grupo que assumiu a autoria do crime por meio do *defacement* do sítio do Ministério[xliv].

238. Em 12/12/2021, o MS publicou nova nota informando "que o processo para recuperação dos registros dos brasileiros vacinados contra a Covid-19 foi finalizado, sem perda de informações"[xlv]. No dia seguinte, o GSI/PR divulgou nota à imprensa informando que "ocorreram

incidentes cibernéticos contra órgãos de Governo em ambiente de nuvem" e que "o CTIR Gov emitiu, em conjunto com a SGD/ME [Secretaria de Governo Digital do Ministério da Economia], o Alerta 08/2021 com medidas mitigadoras e de prevenção sobre o tema"[xlvi].

239. O referido alerta informava que "estão sendo observadas diversas ações maliciosas em ambientes de *Cloud*, como intrusões, *defacement* e exclusão de dados, dentre outras" e que "alguns casos de intrusão têm ocorrido com o uso de perfis legítimos de administrador, o que dispensa, ao atacante, ações para escalar privilégios"[xxxvi].

240. Conforme noticiado na imprensa, a Controladoria-Geral da União (CGU), a Polícia Rodoviária Federal (PRF) e o Instituto Federal do Paraná (IFPR), bem como a própria PF, também haviam sido alvo de ataques na mesma data[xlvii].

241. Somente em 24/12/2021, o Departamento de Informática do SUS (Datasus) informou que havia restabelecido a disponibilidade do ConecteSUS Cidadão, "permitindo a visualização dos dados vacinais e a emissão do Certificado Nacional de Vacinação Covid-19", que "Estados, Municípios e Distrito Federal estão[estavam] aptos a realizarem as notificações de casos suspeitos de Covid-19 e registros dos dados vacinais nas plataformas e-SUS Notifica e SI-PNI", que "o acesso às APIs do Sivep Gripe e Notifica já foram[haviam sido] disponibilizados aos usuários estaduais" e que "não houve perda de dados durante o incidente de segurança, visto que, o [MS] tem um fluxo de backup consolidado"[xlviii].

242. Entretanto, pouco mais de um mês após o ataque, em 12/1/2022, foi noticiado que "o [MS] informou que os sistemas de dados do órgão que ainda não estão disponíveis serão normalizados até sexta-feira (14[/1])", que, "em entrevista coletiva, o secretário executivo do ministério, Rodrigo Cruz, detalhou que, até o final desta semana, devem ser disponibilizados dados sobre vacinação contra a covid-19, além de outras informações que ainda não estão plenamente acessíveis ao público" e que alguns sistemas (*e.g.* LocalizaSUS) e painéis de informação (*e.g.* Open DataSus, painel coronavírus) seguiam "indisponíveis ou com dificuldades na atualização". Nessa mesma entrevista, o Secretário Executivo afirmou que os dados estavam preservados: "Como havia cópia de tudo, não houve perda"[xlix].

243. O incidente evidenciou a importância da implementação dos controles e medidas de segurança avaliados no âmbito deste acompanhamento, em especial quanto à instituição de uma política geral e de procedimentos específicos de *backup* e *restore*, efetivos e adequados às necessidades de negócio da organização, sobretudo em relação aos seus sistemas e dados críticos.

244. Esta unidade técnica, por meio da realização de reuniões remotas com gestores do Datasus e do envio de ofícios de requisição de informações ao MS (Ofícios 2 e 6/2022-TCU/Sefti, de 14/1 e 4/2/2022, respectivamente – peças 798 e 802), acompanhou de perto a situação. No entanto, devido à sensibilidade do incidente e a necessidade de se preservar informações sigilosas, o caso foi analisado em papel de trabalho à parte (peça 854).

245. Conforme proposta consignada naquela análise, tendo em vista a importância e o relevante interesse público do tema e a necessidade de se dar adequada transparência dos trabalhos realizados pelo TCU à sociedade em geral e, em especial, aos parlamentares e aos jornalistas que requereram providências do Tribunal, informa-se que:

245.1. a Sefti analisou o incidente e concluiu que foram adequadas as ações do Ministério da Saúde para a resposta imediata e a recuperação dos sistemas afetados pelo incidente;

245.2. há indicativos de que os sistemas afetados, inclusive o ConecteSus, estão atualizados e operando em situação de normalidade, porém ainda podem eventualmente ocorrer algumas falhas pontuais de baixo impacto;

245.3. foram elaborados planos pelos gestores do Ministério da Saúde com vistas aprimorar a governança e os controles relacionados com a SegCiber do órgão, de modo a prevenir a ocorrência futura de incidentes semelhantes; e

245.4. a Sefti poderá fazer nova avaliação em etapa futura deste acompanhamento para analisar a efetividade dessas ações planejadas pelo MS e para realizar análises complementares.

246. Também em consonância com aquele papel de trabalho, as seguintes propostas de encaminhamento foram incorporadas a este relatório de acompanhamento:

246.1. dar ciência ao Ministério da Saúde, com fundamento no art. 9º, incisos I e II, da Resolução-TCU 315/2020, que a não designação de servidores para compor o comitê de segurança da informação ou estrutura equivalente do órgão ofende ao disposto no art. 15, inciso IV e § 1º, do Decreto 9.637/2018 e no art. 17 da Portaria 271/2017 desse ministério, que dispõe sobre a sua Política de Segurança da Informação e Comunicações, e constitui obstáculo para o atendimento às disposições do art. 8º da Instrução Normativa 5/2021 do Gabinete de Segurança Institucional da Presidência da República;

246.2. encaminhar ao Ministério da Saúde cópia eletrônica do papel de trabalho da análise do incidente de segurança da informação/ataque *hacker* ocorrido em dezembro de 2021 (peça 854), informando que se trata de documento classificado como reservado pelo TCU, para que tome conhecimento das conclusões da análise realizada pela Sefti e das ações que foram identificadas como possíveis medidas complementares para auxiliar na mitigação de eventos futuros semelhantes e elevar a resiliência da organização;

246.3. à luz dos arts. 23 e 24 da Lei 12.527/2011 (Lei de Acesso à Informação), classificar como reservados, por conterem informações consideradas imprescindíveis à segurança da sociedade ou do Estado, o papel de trabalho da análise do incidente de segurança da informação/ataque *hacker* ocorrido no Ministério da Saúde em dezembro de 2021 (peça 854), a peça 811 e os itens não digitalizáveis dessas peças.

Resultados do iGG 2021

247. Desde 2007, o TCU realiza fiscalizações para levantar informações sobre a situação da governança na Administração Pública. Em 2017, foi realizado o primeiro levantamento do Perfil Integrado de Governança Organizacional e Gestão Públicas (TC 017.245/2017-6; Rel. Min. Bruno Dantas)[I], trabalho mais conhecido pela sigla do seu principal indicador, o Índice Integrado de Governança e Gestão Públicas (iGG). Em 2021, foi realizado o ciclo mais recente, no qual foram avaliadas 378 organizações públicas federais (TC 011.574/2021-6; Rel. Min. Bruno Dantas)[II].

248. O iGG reúne, em um só instrumento de autoavaliação, cinco dimensões (governança pública organizacional, gestão de pessoas, gestão de TI, gestão de contratações e gestão orçamentária), o que possibilita uma análise mais ampla da governança e da gestão das organizações avaliadas. Em função dos valores obtidos nesse indicador (e nos demais índices agregadores), as organizações avaliadas são classificadas em quatros estágios progressivos de capacidade de governança organizacional e gestão públicas: Inexpressivo, Inicial, Intermediário e Aprimorado.

249. Para o propósito deste acompanhamento de SegCiber, interessa analisar o Índice de Gestão de Segurança da Informação (iGestSegInfo), que é um dos índices agregadores que compõem o Índice de Gestão de TI (iGestTI), que, por sua vez, é um dos índices agregadores que compõem o iGG. Conforme se vê na Figura 43, o relatório consolidador do iGG 2021 (TC 011.574/2021-6[II], peça 1.060) comparou o iGestSegInfo entre 2018 e 2021, mostrando que a situação da gestão de SegInfo das organizações piorou entre essas duas avaliações.

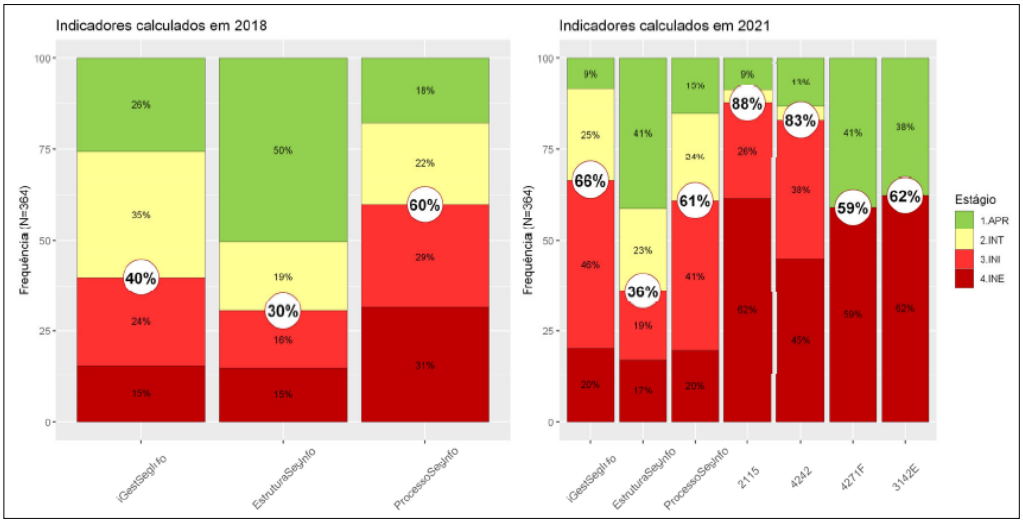



**Figura 43 - Índice de gestão de SegInfo (iGestSegInfo): comparação entre 2018 e 2021.**
(Fonte: TC 011.574/2021-6[li], peça 1.060 [relatório consolidador do iGG 2021], Figura 65)

250. Entretanto, conforme apontado naquele relatório consolidador, percebe-se que houve expressiva mudança nos critérios utilizados para avaliação do iGestSegInfo em 2021:

> 226. (...) A gestão de segurança da informação era mensurada, em 2018, por meio dos seguintes componentes e práticas associadas: estrutura organizacional para a segurança da informação (EstruturaSegInfo) e processos de gestão da segurança da informação (ProcessoSegInfo). No trabalho de 2021, esses componentes foram mantidos e foram acrescentadas ainda práticas relativas às seguintes questões: gestão de continuidade do negócio institucional (2115), gestão de continuidade de serviços de TI (4242), gestão da segurança da informação no processo de software (4271F) e auditoria da gestão da segurança da informação (3142E).
>
> 227. Como se vê na [Figura 43], os indicadores comuns às duas fiscalizações, EstruturaSegInfo e ProcessoSegInfo apresentam pequena redução na capacidade de gestão em 2021. Porém, considera-se que as diferenças observadas na mensuração desses dois componentes entre 2018 e 2021 poderiam ser explicadas por alterações ocorridas nos critérios utilizados no questionário aplicado em 2021.
>
> 228. Quanto aos novos componentes que foram acrescentados à composição do iGestSegInfo em 2021, nota-se nessa figura que a maioria das instituições apresentam grandes deficiências na capacidade de realização das práticas correspondentes, indicando que eles são os principais responsáveis pela degradação observada na mensuração do indicador, que passou de 40% das instituições situadas nos estágios de capacidade iniciais em 2018 para 66% em 2021, considerando-se as 364 organizações que responderam aos dois questionários.

251. Para analisar mais a fundo a situação retratada pelo iGestSegInfo, aquele relatório apresentou, também, um gráfico com a distribuição por estágios de capacidade de todas as 378 organizações avaliadas em 2021 (Figura 44).

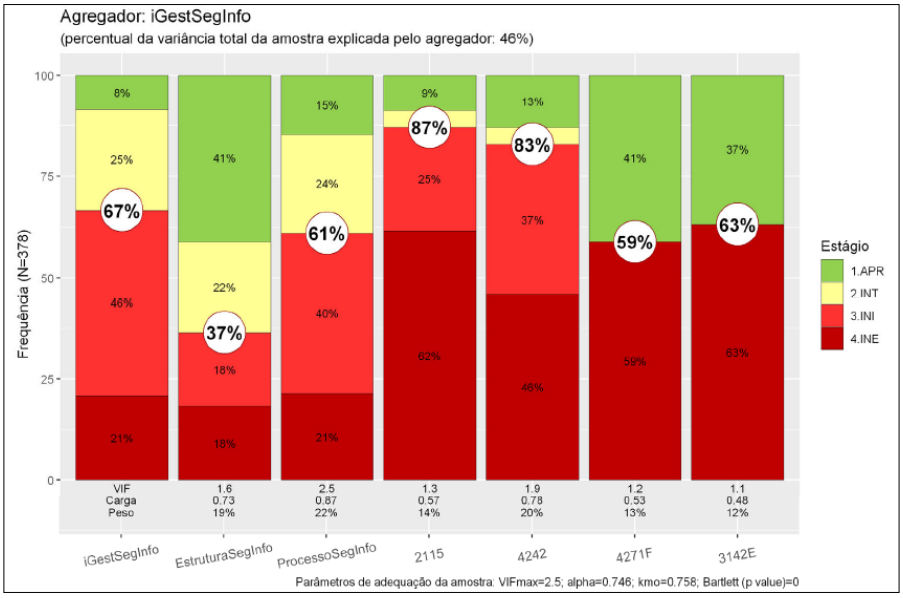



**Figura 44 - Índice de Gestão de SegInfo (iGestSegInfo) 2021.**
(Fonte: TC 011.574/2021-6[li], peça 1.060 [relatório consolidador do iGG 2021], Figura 66)

252. O relatório destacou a situação ruim das gestões de continuidade institucional, de continuidade de serviços de TI, da SegInfo no processo de software e da auditoria da gestão da SegInfo:

> 230. Apesar da situação ruim em todos os novos quesitos adicionados ao iGestSegInfo em 2021, verifica-se na [Figura 44] que os destaques negativos incontestáveis são a gestão de continuidade institucional (questão 2115) e gestão de continuidade de serviços de TI (questão 4242), que apresentam 87% e 83% respectivamente de instituições nos estágios iniciais de capacidade. E, pior ainda, a gestão de continuidade institucional está no estágio de capacidade inexpressivo em 62% das organizações e a gestão de continuidade de serviços de TI é inexpressiva em 46% das organizações avaliadas.
> 231. Importante mencionar também que as práticas relacionadas com a gestão da segurança da informação no processo de software (questão 4271F) e com a auditoria da gestão de segurança da informação (questão 3142E) também se revelam inexpressivas em aproximadamente 60% das organizações. (...)
> (...)
> 234. (...) a gestão da continuidade, em âmbito institucional e de serviços de TI, é imprescindível para assegurar a resiliência e, até mesmo, a própria existência das organizações, atualmente, em face da dependência cada vez maior de informações e de processos automatizados por tecnologias da informação, caso ocorram eventos de difícil prevenção com potencial catastrófico.

253. Ainda, aquela fiscalização evidenciou carências relacionadas à elaboração da Política de Segurança da Informação (PSI), à designação do gestor institucional de SegInfo e à instituição do Comitê de SegInfo (Tabela 25), itens cujo cumprimento é normativamente previsto para os órgãos e entidades da APF (Decreto 9.637/2018 – PNSI[xv], art. 15, incisos II, III e IV, respectivamente; IN GSI/PR 1/2020, arts. 9º, 15, incisos I e II, e 16, incisos I e II), o que levanta preocupações adicionais.

**Tabela 25 - iGG 2021: distribuição das respostas das 378 organizações às questões 4251, 4252 e 4253.**

(Fonte: elaboração própria, a partir da "Tabela de respostas brutas" do iGG 2021, disponível em https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/levantamento-de-governanca.htm)

| Resposta | 4251 | 4252 | 4253 |
|---|---|---|---|
| A organização não adota | 16 | 53 | 68 |
| Há decisão ou plano para adotar | 34 | 47 | 49 |
| A organização adota em menor parte | 23 | 29 | 30 |
| A organização adota parcialmente | 46 | 29 | 47 |
| A organização adota em maior parte ou totalmente | 255 | 208 | 176 |
| Não se aplica | 4 | 12 | 8 |
| **TOTAL** | **378** | **378** | **378** |

4251) A organização dispõe de uma política de segurança da informação
4252) A organização dispõe de comitê de segurança da informação
4253) A organização possui um gestor institucional de segurança da informação

254. Esses destaques merecem reforço em face do recente incidente cibernético sofrido pelo MS, o qual, em tempo de pandemia, causou a indisponibilidade de importantes serviços públicos, a exemplo da notificação de casos de Covid-19 e da emissão do certificado de vacinação. Em tais situações, as organizações precisam contar com um plano de continuidade do negócio, o qual deve definir e documentar procedimentos para orientar os gestores a responder a incidentes de interrupção e a retomar as principais atividades da organização em níveis aceitáveis, dentro de prazos predefinidos.

255. O relatório do iGG 2021, então, considerando "a situação preocupante da capacidade inexpressiva de realização de práticas essenciais de gestão de [SegInfo], de gestão de continuidade do negócio e de continuidade de serviços de TI por metade ou mais das organizações públicas avaliadas", concluiu ser "necessário sistemático acompanhamento dessa situação por parte do TCU, bem como eventual planejamento de ações de controle com o objetivo de verificar mais a fundo e pontualmente essas questões, especialmente em casos de alta materialidade e relevância" (grifos no original).

256. Assim, ante o exposto, esta equipe vislumbra oportuno, também, atualizar e reforçar as ações relacionadas ao iGestSegInfo já previstas na "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023"**Error! Bookmark not defined.** (Figura 39, eixo "Acompanhar"), no sentido de acompanhar a evolução das práticas de gestão de SegInfo e SegCiber pelas organizações públicas federais, em especial de 2021 para a próxima avaliação do iGG, que deve ocorrer em 2023 (periodicidade bienal). Essa atualização será feita no âmbito da "Estratégia de Fiscalização do TCU em SegInfo e Privacidade de Dados 2022-2025" (parágrafo 260).

## 7. Perspectiva para o futuro

257. A "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023" previu a realização de um acompanhamento de controles críticos de SegCiber (Figura 39, Eixo "Diagnosticar"), autorizado por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de *backup* e *restore* dos órgãos e entidades da APF; Rel. Min. Vital do Rêgo) e previsto para acontecer em sete ciclos, ao longo dos próximos anos (Tabela 2, peça 855**Error! Reference source not found.**).

258. Após a execução de cada um desses ciclos, o respectivo relatório apontará os principais registros verificados (o Capítulo 3 traz aqueles relativos ao primeiro ciclo) e, com base neles, fará a proposição de medidas com vistas a contribuir para a melhoria do cenário encontrado (Capítulo 9).

259. Das ações previstas no Eixo "Mapear" daquela estratégia (Figura 39), sugere-se priorizar, pelo seu caráter estruturante, o "Levantamento de infraestruturas críticas nacionais", a ser realizado em conjunto com a Secretaria de Controle Externo da Defesa Nacional e da Segurança Pública (SecexDefesa). E, tendo em vista que, de 2018 para 2020, o Brasil ascendeu da 70ª (TC 001.873/2020-2, peça 46, Figura 1) para a 18ª posição (Figura 45) no *Global Cybersecurity Index* (GCI)[lii], *ranking* de desenvolvimento em SegCiber organizado pela *International Telecommunication Union* (ITU), perdeu importância o "*Benchmarking* internacional", embora sua realização continue sendo prevista, por ora.

| Country Name | Score | Rank |
|---|---|---|
| United States of America* | 100 | 1 |
| United Kingdom | 99.54 | 2 |
| Saudi Arabia | 99.54 | 2 |
| Estonia | 99.48 | 3 |
| Korea (Rep. of) | 98.52 | 4 |
| Singapore | 98.52 | 4 |
| Spain | 98.52 | 4 |
| Russian Federation | 98.06 | 5 |
| United Arab Emirates | 98.06 | 5 |
| Malaysia | 98.06 | 5 |
| Lithuania | 97.93 | 6 |
| Japan | 97.82 | 7 |

| Country Name | Score | Rank |
|---|---|---|
| Canada* | 97.67 | 8 |
| France | 97.6 | 9 |
| India | 97.5 | 10 |
| Turkey | 97.49 | 11 |
| Australia | 97.47 | 12 |
| Luxembourg | 97.41 | 13 |
| Germany | 97.41 | 13 |
| Portugal | 97.32 | 14 |
| Latvia | 97.28 | 15 |
| Netherlands* | 97.05 | 16 |
| Norway* | 96.89 | 17 |
| Mauritius | 96.89 | 17 |
| Brazil | 96.6 | 18 |

* no response to the questionnaire

**Figura 45 - *Ranking* de desenvolvimento dos países em termos de SegCiber.**
(Fonte: *Global Cybersecurity Index* 2020[lii])

260. A estratégia de fiscalização original será atualizada e publicada em documento apartado, sob o nome "Estratégia de Fiscalização do TCU em SegInfo e Proteção de Dados 2022-2025", passando a incluir, também, as ações e fiscalizações relativas às áreas de privacidade e proteção de dados pessoais, que adquiriram maior relevância a partir das promulgações da Lei 13.709/2018 (LGPD)[x] e da recente Emenda Constitucional (EC) 115[liii], que incluiu essa proteção entre os direitos e garantias fundamentais previstos na Constituição Federal. Inclusive, já foi realizada a "Auditoria sobre a LGPD" (TC 039.606/2020-1 - Rel. Min. Augusto Nardes[ix]; Figura 39, Eixo "Diagnosticar"; parágrafo 12).

261. Conforme adiantado no início deste relatório (Tabela 2, peça 855), no segundo ciclo de execução do acompanhamento serão avaliados, adicionalmente aos controles já verificados neste ciclo, os seguintes: 4) Configuração segura de ativos corporativos e de software; 5) Gestão de contas; 6) Gestão de controles de acesso; 9) Proteções de *e-mail* e de navegador da *web*; e 10) Defesas contra *malware*. Além disso, também serão avaliadas as medidas de segurança intermediárias (IG2) dos controles 1 (Inventário e controle de ativos corporativos) e 2 (Inventário e controle de ativos de software).

262. A seu turno, no terceiro ciclo serão avaliados, adicionalmente a todos os anteriores (deste e do segundo ciclos), os seguintes controles: 3) Proteção de dados; 8) Gestão de registros (*logs*) de auditoria; 11) Recuperação de dados; 12) Gestão de infraestrutura de rede; e 13) Monitoramento e defesa de rede. Nesse ciclo, além de passarem a ser avaliadas as medidas de segurança intermediárias (IG2) dos controles 7 (Gestão contínua de vulnerabilidades) e 17 (Gestão de respostas a incidentes), será possível aferir a evolução ocorrida em relação aos controles de *backup*/*restore* desde a auditoria-piloto que desencadeou a realização deste acompanhamento (TC 036.620/2020-3; Rel. Min. Vital do Rêgo)[viii].

263. Ao longo do tempo, o painel construído (Capítulo 4) poderá absorver os resultados de outras fiscalizações da Corte, permitindo correlacionar, para organizações individuais ou para conjuntos de organizações (Anexo III, peça 855), como estas/estes se encontram em relação a múltiplas dimensões de interesse, o que possibilitará realizar interessantes análises, a exemplo de algumas já trazidas, inclusive, no bojo deste primeiro ciclo (Figuras 36 e 37).

264. Ademais, relativamente às fiscalizações que ocorrerão de maneira periódica (*e.g.* este acompanhamento, Levantamento Integrado de Governança Organizacional Pública), o painel poderá permitir a guarda do histórico dos dados derivados das respostas das organizações às várias aplicações dos questionários ao longo do tempo, possibilitando, assim, que sejam gerados gráficos da evolução da capacidade das organizações em relação a tais dimensões de interesse. No que se refere a esta fiscalização, por exemplo, será possível acompanhar a gradativa evolução da maturidade das organizações em relação à implementação dos controles críticos de SegCiber.

265. Convém, ainda, citar iniciativas de outros órgãos que guardam relação com os objetivos deste acompanhamento. A SGD/ME, por exemplo, publicou os "Guias operacionais para adequação à LGPD"[liv] e, em resposta ao Acórdão 1.889/2020-TCU-Plenário (TC 031.436/2019-6, levantamento de riscos em sistemas informacionais da APF; Rel. Min. Aroldo Cedraz)[lv], está conduzindo o Programa de Privacidade e Segurança da Informação (PPSI), visando a "elevar o grau de maturidade, em termos de proteção de dados pessoais e sensíveis e ações de [SegInfo], dos órgãos integrantes do SISP [Sistema de Administração dos Recursos de Tecnologia da Informação], aumentando a proteção dos sistemas críticos de governo no ambiente cibernético" (peça 805, p. 1).

266. Em reuniões realizadas nos dias 12 e 19/1/2022, representantes do TCU, do GSI/PR e da ANPD foram convidados a apresentar brevemente suas visões relacionadas às áreas de privacidade e SegInfo (peça 805, p. 2-3). O GSI vem revisando os normativos já publicados e publicando novos, além de estar elaborando as minutas de um Projeto de Lei para tratar da Política Nacional de Segurança Cibernética (PNSC), bem como dos Planos Nacionais de Segurança das Infraestruturas Críticas (PLANSIC) e de Gestão de Incidentes Cibernéticos (PLANGIC) e dos correspondentes planos setoriais. Estes últimos deverão dar mais concretude à implementação da REGIC na APF (Decreto 10.748/2021[xvi]).

267. A ANPD, a seu turno, tem estreitado seu relacionamento com outros entes nacionais (*e.g.* agências reguladoras), bem como firmado diversos acordos de cooperação técnica (inclusive com a Autoridade Espanhola de Proteção de Dados – AEPD) voltados à realização de ações de fiscalização e à elaboração conjunta de materiais orientativos, estudos e outras publicações[lvi]. O órgão também intensificou o diálogo com autoridades e organizações estrangeiras e vem gradativamente se inserindo em debates e fóruns internacionais, tais como a *Global Privacy Enforcement Network* (GPEN)[lvii], a *Global Privacy Assembly* (GPA)[lviii], a *Convention 108 on Data Protection* do *Council of Europe*[lix], a Rede Ibero-americana de Proteção de Dados (RIPD)[lx] e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE)[lxi].

268. Por fim, sugere-se que, após a execução de cada um dos ciclos deste acompanhamento, a Sefti elabore e publique documento técnico visando a orientar os gestores quanto à implementação dos controles críticos e medidas de segurança do *framework* do CIS avaliados naquele ciclo, atualizando progressivamente tal documento, de modo similar ao que vem realizando a agência americana (*Cybersecurity & Infrastructure Security Agency* – CISA)[lxii].

## 8. Comentários dos gestores

269. Em consonância com o disposto no art. 14 da Resolução-TCU 315/2020, a versão preliminar deste relatório (peça 819) foi enviada para receber comentários dos gestores das seguintes organizações destinatárias de propostas de deliberações: Secretaria de Governo Digital do Ministério da Economia (peça 822), Supremo Tribunal Federal (peça 823), Conselho Nacional de Justiça (peça 824), Conselho Nacional do Ministério Público (peça 825), Tribunal de Contas da União (peça 827), Gabinete de Segurança Institucional da Presidência da República (peça 828), Câmara dos Deputados (peça 832) e Senado Federal (peça 833).

270. Os comentários são a oportunidade para que os gestores apresentem suas perspectivas sobre as questões levantadas neste relatório e informações sobre as consequências práticas da implementação das deliberações aventadas, bem como sugestões de eventuais medidas alternativas.

271. Cabe ressaltar que decorridos os prazos para o pronunciamento facultativo dos gestores, apenas Câmara dos Deputados e Supremo Tribunal Federal não se manifestaram. A seguir, serão analisados os comentários recebidos das demais organizações.

Conselho Nacional do Ministério Público (CNMP) - peças 834 e 835

272. Em especial, os gestores do CNMP se manifestaram de forma destacada (peça 834) no sentido de que a recomendação do item 280.3 "parece remeter à interpretação desta unidade técnica do TCU quanto ao enquadramento do CNMP como Órgão Governante Superior (OGS)", conceito este que já foi refutado em decisão plenária proferida por aquele Conselho em 14/6/2016 (peça 835).

273. De fato, a equipe de fiscalização tinha endereçado a recomendação considerando que o CNMP exerceria o papel de OGS, pois executa a fiscalização administrativa, financeira e disciplinar de todos os ramos do Ministério Público no Brasil.

274. No entanto, considerando que o CNMP não reconhece esse papel, a recomendação será redirecionada diretamente para cada um dos ramos do Ministério Público da União (MPU): Ministério Público Federal (MPF), Ministério Público Militar (MPM), Ministério Público do Trabalho (MPT) e Ministério Público do Distrito Federal e Territórios (MPDFT).

Conselho Nacional de Justiça (CNJ) - peças 837 e 838

275. Em sua manifestação (peça 838), os gestores do CNJ sugerem: "(...) a indicação pela Corte de Contas de boas práticas, modelos, referências e demais artefatos (acórdãos, estudos técnicos, termos de referência) que funcionem como facilitadores para a contratação de soluções e serviços de TIC de forma célere e internamente pacificada (...)"; "(...) que seja criado um índice de capacidade de prontidão/resposta aos riscos de segurança da informação, a partir dos critérios de existência de área específica de SegInfo, da quantidade de técnicos dedicados e treinados, bem como do nível de cultura das áreas usuárias de TIC neste quesito"; e "(...) que no próximo ciclo de monitoramento seja perscrutada a situação dos entes públicos no que se refere aos recursos humanos disponíveis, exclusivamente ou não".

276. Com relação à primeira sugestão, ressalva-se que o tema de contratação de soluções e serviços de TIC foge ao escopo deste acompanhamento, mas se destaca que é objeto do "Guia de boas práticas em contratação de soluções de tecnologia da informação: riscos e controles para o planejamento da contratação", publicado pelo TCU em 2012[lxiii], e do "Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação", publicado pela antiga Secretaria de Tecnologia da Informação e Comunicação do Ministério do Planejamento, Desenvolvimento e Gestão em 2017[lxiv].

277. Quanto às demais sugestões, destaca-se que já foi calculado e está sendo proposto neste relatório o índice de maturidade em SegCiber (iSegCiber) com base nos controles avaliados neste primeiro ciclo do acompanhamento (capítulo 5 - tópico "Indicadores de SegCiber") e que já foi calculado o Índice de Gestão de SegInfo (iGestSegInfo) no âmbito do IGG 2021 (capítulo 6 – tópico "Resultados do iGG 2021").

278. Assim, a sugestão de incluir critérios de avaliação relacionados com recursos humanos em segurança da informação já está parcialmente atendida com a inclusão do Controle 14 (Conscientização sobre segurança e treinamento de competências) do CIS neste primeiro ciclo, sem prejuízo de ser levada em consideração integralmente no planejamento do próximo ciclo do acompanhamento; e a sugestão sobre incluir a existência de área específica de SegInfo já está atendida por meio de quesito específico no questionário do IGG. Restaria então avaliar, também no próximo ciclo, a possibilidade de consolidar os dois indicadores (iSegCiber e iGestSegInfo) em um índice geral de SegInfo.

279. Desse modo, as sugestões apresentadas pelo CNJ não demandaram alteração no relatório e nas propostas de encaminhamento deste ciclo do acompanhamento.

Gabinete de Segurança Institucional da Presidência da República (GSI/PR) - peças 839 e 840

280. Em sua manifestação (peça 840), os gestores do GSI/PR pediram mudança na redação do texto do item 280.1.1 do relatório preliminar, com base nos seguintes argumentos:

> a) O GSI, ao publicar a IN GSI/PR 01/2020 e a IN GSI/PR 03/2021, já definiu a estrutura mínima de gestão de segurança cibernética e os processos mínimos relativos à segurança cibernética que os órgãos devem possuir, entre eles o mapeamento de ativos, gestão de riscos, planejamento de contingência e continuidade de negócios, gestão de mudanças e avaliação de conformidade. Nesses documentos já se define o que deve ser feito e se recomenda a adoção das melhores práticas relativas ao assunto.
>
> b) O GSI já observa, na elaboração de suas normas, os principais *frameworks* e práticas relativas à segurança cibernética, e tem tido o cuidado de solicitar apenas os requisitos mínimos em função do nível de maturidade e das particularidades dos órgãos e das entidades da Administração Pública Federal, em termos de governança da segurança cibernética;
>
> c) Apesar de reconhecer a abrangência dos CIS Controls V8, que é a última versão disponibilizada pelo Center for Internet Security, entendemos que existem outros *frameworks* e práticas que também são capazes de cumprir com as necessidades de segurança cibernética. (...) Consideramos, portanto, que o mais adequado seria indicar os principais *frameworks* e práticas, deixando a escolha do(s) modelo(s) por conta do órgão ou da entidade em função de sua capacidade operacional e de sua maturidade para implementar os procedimentos de segurança cibernética necessários.
>
> d) Entendemos que, como órgão normatizador, cabe ao GSI determinar apenas 'o que deve ser feito', ficando a cargo do órgão ou da entidade da Administração Pública federal (APF) definir a melhor maneira 'de como deve ser feito', evitando dessa forma uma maior ingerência nas atividades dos órgãos e das entidades da APF. Baseado nesse entendimento, consideramos que a elaboração de guias deveria ser uma atividade da SGD/ME (...).
>
> e) Por fim, impor tão-somente o modelo preconizado pelo CIS poderia implicar em custos adicionais para diversos órgãos e entidades da APF que já adotaram outros frameworks de segurança e que seriam obrigados a fazer diversas adequações para ficar em conformidade com apenas esse modelo. Isso inclusive implicaria na obrigatoriedade da migração do CIS v7, com seus 20 controles, para o CIS v8, com 18 controles.

281. Em primeiro lugar, é preciso salientar que este acompanhamento foi construído com base nos controles do CIS porque este é um *framework* mais técnico e específico para segurança cibernética. No entanto, conforme já foi citado neste relatório (parágrafo 17), realmente existem diversos outros critérios normativos que também dão suporte aos controles e às medidas de segurança avaliadas, sendo que alguns deles – incluindo as próprias normas do GSI/PR e outras referências que foram citadas por seus gestores – foram utilizados como critérios para os principais registros deste ciclo do acompanhamento (capítulo 3). Assim, ao implementar os controles recomendados, as organizações podem e devem utilizar outros *frameworks* como referência, não apenas o CIS.

282. Também é preciso destacar que os controles do CIS formam um conjunto de ações de defesa de alta prioridade contra os ataques cibernéticos mais pervasivos, foram desenvolvidos por uma comunidade global de TI e são utilizados no mundo todo. Diante do cenário atual de ameaças crescentes, inclusive de guerra cibernética, e da situação retratada neste relatório, esses controles são ações consideradas imprescindíveis e urgentes para toda organização que busca melhorar a sua segurança cibernética.

283. Ainda assim, neste primeiro ciclo do acompanhamento somente foram questionadas medidas de segurança consideradas básicas dentre os controles avaliados. Os demais controles e medidas de segurança preconizadas pelo CIS serão progressivamente avaliadas pelo TCU ao longo de sete ciclos. De todo modo, as organizações devem avaliar, decidir e priorizar quais controles implementar em função do cenário de riscos a que seu negócio está exposto.

284. Ademais, é preciso destacar que a situação retratada neste acompanhamento também é um indicativo de que as diversas normas do GSI/PR não estão de fato sendo observadas pelos órgãos

e entidades da APF. Assim, a proposta do item 280.1.1 foi elaborada no sentido de fortalecer a atuação do GSI/PR também quanto à indução, monitoramento e avaliação do cumprimento efetivo de seus normativos.

285. Quanto ao papel orientador da SGD/ME, incluindo a elaboração de normativos e guias, ressalva-se que seu alcance é restrito de forma obrigatória apenas aos órgãos participantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo Federal.

286. Portanto, o que se percebe é que permanece a situação apontada no relatório do levantamento da governança e gestão SegInfo e de SegCiber na APF (001.873/2020-2, de relatoria do Min. Vital do Rêgo) em que a macroestrutura nacional responsável pela governança e gestão das questões de SegInfo/SegCiber, apesar de atuante, não se mostrava adequada, dados os alcances limitados da atuação do seu principal órgão (GSI/PR) e da regência do atual arcabouço normativo, que não alcançam a Administração Pública como um todo, mas apenas o Poder Executivo federal.

287. Diante do exposto, decidiu-se excluir a proposta de encaminhamento correspondente ao item 280.1.1 do relatório preliminar, que era endereçada ao GSI/PR, e fazer ajustes na redação original da proposta do item 280.2, que é endereçada à SGD/ME.

Tribunal de Contas da União (TCU) - peça 841

288. Em sua manifestação (peça 841, grifo nosso), o Secretário-Geral da Presidência do TCU apenas informou que:

> (...) após análise das áreas envolvidas com a matéria, entendeu-se que os encaminhamentos propostos se alinham à direção adotada pelo TCU quanto à adoção dos controles CIS (*Critical Security Controls*) para priorização de ações de segurança e diagnóstico de maturidade. Dessa forma, não se identificou necessidade de tecer comentários ao mencionado relatório.

289. Portanto, a manifestação do TCU não demandou alteração no relatório e nas propostas de encaminhamento deste ciclo do acompanhamento.

Senado Federal - peças 845,846 e 847

290. Da manifestação dos gestores do Senado Federal (peça 846), destacam-se os seguintes pontos (grifos nossos):

> (...)
>
> 2. Primeiramente, cumpre ressaltar a qualidade e extrema importância do trabalho realizado pela Corte de Contas neste acompanhamento de tema tão prioritário para as organizações, sejam públicas ou privadas. O arranjo em etapas (ciclos) da proposta tem o condão de elevar a maturidade dos auditados no tema alvo. Em verdade, conforme asseverado pelo Tribunal no referido relatório, a Administração Pública Federal tem se esforçado para promover a Transformação Digital (TD) dos serviços públicos. No entanto, a concentração de esforços nessa nobre e legítima missão, considerando a limitação de recursos apontada pelos respondentes, resta por deixar a segurança da informação (SegInfo) e a segurança cibernética (SegCiber) em segundo plano.
>
> 3. Conforme manifestado pelos fiscalizados, o desafio da segurança cibernética encontra-se em grande parte na falta de pessoal ou na falta de pessoal especializado, na capacitação – tanto de técnicos quanto de usuários -, na gestão e nos normativos de SegInfo e SegCiber, e nos orçamentos para aquisições no campo da infraestrutura tecnológica. Basicamente, pode-se conectar essas respostas aos pilares da organização do trabalho: pessoas, processos, estruturas e tecnologias.
>
> 4. E os achados dos auditores, em grande parte tidos como preocupantes por aquela equipe, não deixam de ter um efeito vinculante aos fiscalizados no sentido da ação célere quanto às propostas de determinação e, não menos importante, às recomendações.

291. Os gestores também teceram comentários de forma tabular que, em síntese, concordavam com as propostas de encaminhamento exaradas no relatório preliminar. Dentre esses comentários, destaca-se o seguinte (grifos nossos):

> Quando é necessário estruturar determinado tema organizacional ou processo, recorre-se a modelos nacionais, ou internacionais, que prescrevem um caminho ordenado para o sucesso da empreitada. Normas e Modelos de Maturidade expedidos por entidades de renome, tais como a ABNT (Associação Brasileira de Normas Técnicas) ou a ISO (*International Organization for Standardization*), conduzem as organizações, nos mais variados temas, a melhorias em seus processos internos. Entendemos que com o CIS (*Center for Internet Security*) não é diferente. O Senado Federal, em seu recente ciclo de revisão e atualização (2021/2022) do Planejamento Estratégico Institucional, incluiu entre os seus objetivos e resultados-chave a elaboração de um Plano de Ação em Segurança Cibernética, cuja corrente elaboração será enriquecida, tendo como norte o modelo CIS. Nesse sentido, o CSI (Comitê de Segurança da Informação) do Senado Federal envidará esforços junto aos provedores de Tecnologia da Informação desta Casa no sentido da implementação célere do referido plano.

292. Portanto, a manifestação do Senado Federal também não demandou alteração no relatório e nas propostas de encaminhamento deste ciclo do acompanhamento.

Secretaria de Governo Digital do Ministério da Economia (SGD/ME) - peças 848 e 849

293. A manifestação dos gestores da SGD/ME (peça 849) apresentou análise das iniciativas que atualmente já contribuem com os controles críticos citados no relatório preliminar deste acompanhamento, "para que posteriormente sejam estudadas as possíveis oportunidades de elaboração de novos normativos ou guias, e caso necessário sejam realizadas melhorias ou ajustes no texto dos normativos existentes (...).

294. Os gestores registraram que a SGD/ME vem atuando desde 2020 no sentido de aprimorar a proteção de dados pessoais e a segurança da informação das plataformas de governo digital e dos sistemas críticos do governo federal. Tal atuação, até o ano de 2021, estava estruturada em três frentes: "em amplitude, mediante a divulgação dos guias operacionais de privacidade e segurança da informação"; "em profundidade, com o acompanhamento da equipe da Secretaria, junto aos órgãos detentores de sistemas de missão crítica, para diagnóstico e implementação de controles de privacidade e segurança"; e "em planos de transformação digital, fomentando a inclusão do eixo "Privacidade e Segurança" nos planos de transformação digital dos órgãos do SISP".

295. Os guias editados foram elaborados "buscando fornecer à Administração Pública Federal orientação quanto à adoção das melhores práticas em termos de proteção de dados pessoais e segurança da informação", utilizando "conceitos e recomendações de instituições de referência no setor de segurança da informação", como ABNT, NIST (*National Institute of Standards and Technology*), GSI/PR, ANPD, e o próprio CIS.

296. De acordo com os gestores, mais recentemente a atuação da SGD/ME se desdobrou na implementação de um conjunto de ações estruturadas em um Programa de Privacidade e Segurança da Informação (PPSI), cuja implementação:

> tem como pano de fundo o aprimoramento contínuo das ações da SGD[/ME] face aos desafios encontrados junto aos órgãos da APF na área de privacidade e segurança da informação (...) e é resultado do conjunto de recomendações e achados do TCU no bojo de sua Estratégia de Fiscalização em Segurança da Informação e Segurança Cibernética para o período de 2020-2023 na qual se destacam um conjunto de acórdãos basilares: Acórdão 1.889/2020-TCU-Plenário (Auditoria sobre Sistemas Informacionais Críticos), Acórdão 1.109/2021-Plenário (Auditoria sobre Backups) e Acórdão 1.784/2021-Plenário (Auditoria sobre Estratégias de Transformação Digital da Administração Pública).

297. No contexto das atividades já desenvolvidas pelo PPSI desde o seu lançamento, os gestores destacaram a recente disponibilização de três modelos de controles essenciais baseados nas medidas de segurança cibernética preconizadas pelo CIS: política de *backup*, política de gestão de ativos e política de controle de acesso.

298. Assim, os gestores concluíram, em síntese, que a recomendação para que a SGD/ME edite normativos e guias de forma a orientar os órgãos e entidades participantes do SISP na implementação dos controles preconizados pelo CIS já vem sendo seguida nos últimos anos, tendo ganhado ênfase

recente com a adoção do PPSI, e que "será possível encontrar oportunidades de melhoria e pontos de atenção nesse processo, de forma a melhorar e ajustar o texto dos atuais normativos e guias ou até mesmo realizar a elaboração de novos, caso necessário (...)".

299. Dessa forma, os gestores não apresentaram sugestões ao relatório preliminar da fiscalização, apenas solicitaram acesso integral aos resultados atuais e futuros deste acompanhamento de controles críticos de segurança cibernética.

300. O compartilhamento com a SGD/ME dos dados das respostas individuais das organizações sob sua jurisdição (órgãos e entidades do Sisp) já está incluído nas propostas de encaminhamento deste relatório (item 315.8.1).

301. Apesar de os gestores não terem apresentadas sugestões ao relatório preliminar, um pequeno ajuste foi realizado na redação da proposta de encaminhamento endereçada à SGD/ME (item 315.2), em consideração às ações já realizadas no âmbito do PPSI.

## 9. Conclusão

302. Este primeiro ciclo do acompanhamento objetivou avaliar a implementação, pelas organizações públicas federais, de vinte medidas de segurança básicas (IG1) relacionadas a cinco dos dezoito controles críticos de SegCiber previstos no *framework* do CIS, a saber: 1) Inventário e controle de ativos corporativos; 2) Inventário e controle de ativos de software; 7) Gestão contínua de vulnerabilidades; 14) Conscientização sobre segurança e treinamento de competências; e 17) Gestão de respostas a incidentes (ver Tabela 1).

303. Com esse propósito, foi elaborado e disponibilizado um questionário *online* para ser respondido por gestores de 377 organizações (Anexo I, peça 855**Error! Reference source not found.**). Para cada medida de segurança, foram feitas duas perguntas: uma primeira questionava o grau de adoção daquela medida na organização e uma segunda, então, instava o gestor a marcar as subpráticas específicas, relativas àquela medida, que se encontram efetivamente implementadas na sua organização. Após essas quarenta perguntas (duas perguntas para cada uma das vinte medidas de segurança avaliadas), uma última pergunta solicitava o registro, pelos respondentes, dos principais desafios, deficiências e pontos de atenção relacionados à implantação desses controles, bem como outras considerações, comentários ou críticas que eles considerassem pertinentes.

304. A partir das respostas fornecidas pelos gestores ao questionário, condensadas no Capítulo 2, foi possível realizar análises gerais acerca da implementação desses controles e medidas de segurança no âmbito das organizações avaliadas (Capítulo 3), com a utilização de um painel (*dashboard*) construído exatamente para isso (Capítulo 4).

305. Quanto aos dois primeiros controles (Inventários de ativos de hardware e de software), consideram-se altos os percentuais de organizações que não tratam adequadamente os ativos de hardware não autorizados, corrigindo-os ou removendo-os das suas redes (210 de 377: 55,7%), ou os softwares não autorizados detectados, desinstalando-os dos dispositivos e/ou bloqueando a sua execução (169 de 377: 44,8%), por tais medidas serem básicas. Frise-se que, mesmo entre as organizações que afirmaram tratar esses ativos não autorizados, a frequência desse tratamento é inferior à desejável.

306. O risco dessa ausência de tratamento reside no fato de que tais ativos aumentam a superfície de ataque da organização, podendo ser utilizados por atacantes como vetores para a realização de ações maliciosas, com danos potenciais diversos (*e.g.* indisponibilidade/perda da integridade de sistemas e informações, violação/vazamento de dados, prejuízos financeiros, à credibilidade ou à imagem).

307. No que tange ao controle das vulnerabilidades, consideram-se baixos os percentuais de organizações que mantêm processos ativos para sua gestão (162 de 377: 43%) ou correção (201 de 377: 53,3%), atuando para detectá-las e corrigi-las antes que possam ser exploradas por atacantes. E, mesmo entre as organizações que implementam essas medidas, a minoria aprovou formalmente tais

processos, definiu os papéis e responsabilidades associados e os revisa/atualiza com a periodicidade adequada.

308. De positivo, identificou-se que 77,2% (291 de 377) das organizações automatizam a gestão da aplicação de correções em sistemas operacionais, sendo que a maioria disse utilizar ferramentas para verificar automaticamente a existência desses *patches* ao menos mensalmente, além de monitorar fontes de informações públicas e privadas em busca de ameaças, vulnerabilidades e medidas mitigatórias. Essas práticas reduzem a janela de oportunidade para a exploração das vulnerabilidades nesses ativos.

309. Entre os cinco controles avaliados, a conscientização e capacitação dos colaboradores em SegInfo/SegCiber mostrou cenário preocupante, com deficiências de treinamento relacionadas a todas as medidas de segurança associadas (em especial quanto à identificação e à notificação da falta de atualizações nos ativos e sobre os riscos de conexão e transmissão de dados por meio de redes inseguras), bem como a várias das suas práticas (*e.g.* técnicas de engenharia social, requisitos de segurança de cargos específicos, deleção/descarte seguro de arquivos/mídias/equipamentos, protocolos de criptografia).

310. Por fim, relativamente à gestão de respostas a incidentes, somente 47,5% (179 de 377) das organizações afirmaram manter processo adequado para o recebimento de notificações e, mesmo entre aquelas que disseram adotar tal medida, a maioria não revisa esse processo com a frequência adequada.

311. Por meio da correlação entre os indicadores usados para aferir a maturidade das organizações em gestão de SegInfo e quanto à implementação de controles críticos de SegCiber (Figura 35), foi possível mostrar que as fragilidades identificadas (sintetizadas no Anexo IV, peça 855**Error! Reference source not found.**), de modo geral, decorrem da imaturidade das organizações nesse primeiro quesito, com várias causas possíveis, a exemplo do apoio insuficiente da alta administração e de restrições e carências relacionadas à disponibilidade orçamentária, de recursos humanos e de capacitações/treinamentos.

312. De modo a contribuir para a melhoria do cenário encontrado, esta equipe propõe a edição de normativos específicos para orientar os gestores e fomentar, nas organizações públicas federais, uma rápida e gradativa implementação dos controles críticos e medidas de SegCiber preconizados no *framework* do CIS, priorizando o endereçamento das deficiências e fragilidades mencionadas.

313. Por oportuno, convém reforçar que este acompanhamento objetiva conscientizar e orientar os gestores quanto aos riscos relativos à ausência/deficiência dos controles e medidas de segurança questionados, entendendo-se, portanto, que, mesmo antes da edição de tais normas, as organizações devem se organizar e, proativamente, suprir essas falhas, sob pena de acabarem enfrentando situações similares àquelas enfrentadas pelos órgãos que sofreram ataques cibernéticos recentes (Capítulo 6).

314. Por fim, as organizações podem se preparar para a realização das ações a serem descritas na "Estratégia de Fiscalização do TCU em SegInfo e Privacidade de Dados 2022-2025" (Capítulo 7) e para, ao longo dos próximos ciclos de execução deste acompanhamento, serem verificadas em relação aos demais controles e medidas de segurança do *framework* do CIS, de acordo com a priorização já exposta (Tabela 2, peça 855**Error! Reference source not found.**), sem embargo da eventual necessidade de ajustes e reavaliações ou da realização de auditorias em órgãos ou grupos de órgãos específicos para a verificação *in loco* dos controles informados.

## 10.Propostas de encaminhamento

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

315.1. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, ao Gabinete de Segurança Institucional da Presidência da República que, relativamente à Rede Federal de Gestão de Incidentes Cibernéticos (Decreto 10.748/2021), se ainda não o tiver feito:

315.1.1. envie aos órgãos e entidades da Administração Pública federal ofícios cobrando as respectivas adesões obrigatórias em decorrência do § 1º do art. 1º;

315.1.2. envie às empresas públicas e às sociedades de economia mista federais ofícios sugerindo as respectivas adesões voluntárias, nos termos do § 2º do art. 1º;

315.1.3. envie às pessoas jurídicas de direito público interno dos Poderes Legislativo e Judiciário Federais (este último, por intermédio do Conselho Nacional de Justiça) e do Ministério Público da União, bem como a pessoas jurídicas de direito privado e a outras pessoas jurídicas de direito público (*e.g.* de entes federativos) consideradas relevantes para a formação dessa rede, ofícios sugerindo as respectivas adesões voluntárias, nos termos do § 4º do art. 7º;

315.2. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, à Secretaria de Governo Digital do Ministério da Economia que, como órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo federal, continue a edição de normativos e guias, no âmbito de seu Programa de Privacidade e Segurança da Informação, a fim de orientar os órgãos e entidades participantes desse sistema a implementarem com urgência controles críticos e medidas de segurança cibernética, de modo a tratar, em especial, as deficiências apontadas neste ciclo do acompanhamento, naquilo que lhes for aplicável, observando as normas exaradas pelo Gabinete de Segurança Institucional da Presidência da República e boas práticas como as preconizadas pelo *Center for Internet Security* e pela norma técnica ABNT NBR ISO/IEC 27002:2013;

315.3. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, ao Senado Federal, à Câmara dos Deputados, ao Tribunal de Contas da União, ao Supremo Tribunal Federal, ao Ministério Público Federal, ao Ministério Público Militar, ao Ministério Público do Trabalho e ao Ministério Público do Distrito Federal e Territórios que adotem as ações a seguir; bem como ao Conselho Nacional de Justiça, como órgão governante superior do Poder Judiciário, que edite normativos e guias para orientar os tribunais sob sua jurisdição administrativa a adotá-las:

315.3.1. implementar com urgência controles críticos e medidas de segurança cibernética, de modo a tratar, em especial, as deficiências apontadas neste ciclo do acompanhamento, naquilo que lhes for aplicável, observando boas práticas como as preconizadas pelo *Center for Internet Security* e pela norma técnica ABNT NBR ISO/IEC 27002:2013;

315.3.2. adotar, na inexistência de normativo próprio tratando desses temas, as práticas previstas nos Decretos 9.637/2018 e 10.222/2020, que regem aspectos gerais relacionados à segurança da informação e à segurança cibernética no âmbito da Administração Pública federal, bem como nas instruções normativas e normas complementares editadas pelo Gabinete de Segurança Institucional da Presidência da República (https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao);

315.3.3. formalizar, junto ao Gabinete de Segurança Institucional da Presidência da República, ato de adesão à Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do § 4º do art. 7º do Decreto 10.748/2021;

315.4. 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 as recomendações contidas nos itens anteriores;

315.5. dar ciência ao Ministério da Saúde, com fundamento no art. 9º, incisos I e II, da Resolução-TCU 315/2020, que a não designação de servidores para compor o comitê de segurança da informação ou estrutura equivalente do órgão ofende ao disposto no art. 15, inciso IV e § 1º, do Decreto 9.637/2018 e no art. 17 da Portaria 271/2017 desse ministério, que dispõe sobre a sua Política de Segurança da Informação e Comunicações, e constitui obstáculo para o atendimento às disposições do art. 8º da Instrução Normativa 5/2021 do Gabinete de Segurança Institucional da Presidência da República;

315.6. encaminhar cópias eletrônicas deste relatório e do acórdão decorrente desta fiscalização, bem como do relatório e do voto que fundamentarem este último, ao Gabinete de Segurança Institucional da Presidência da República; à Secretaria de Governo Digital do Ministério da

Economia; à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática e à Presidência do Senado Federal; à Comissão de Ciência e Tecnologia, Comunicação e Informática e à Presidência da Câmara dos Deputados; ao Tribunal de Contas da União; ao Supremo Tribunal Federal; ao Conselho Nacional de Justiça; ao Ministério Público Federal; ao Ministério Público do Trabalho; ao Ministério Público Militar; ao Ministério Público do Distrito Federal e Territórios; bem como às demais organizações públicas federais auditadas;

315.7. encaminhar ao Ministério da Saúde cópia eletrônica do papel de trabalho da análise do incidente de segurança da informação/ataque *hacker* ocorrido em dezembro de 2021 (peça 854), informando que se trata de documento classificado como reservado pelo TCU, para que tome conhecimento das conclusões da análise realizada pela Secretaria de Fiscalização de Tecnologia da Informação e das ações que foram identificadas como possíveis medidas complementares para auxiliar na mitigação de eventos futuros semelhantes e elevar a resiliência da organização;

315.8. autorizar a Secretaria de Fiscalização de Tecnologia da Informação, a fim de alavancar a maturidade das organizações públicas federais relativamente à gestão de segurança cibernética e observada eventual necessidade de despersonificação e de reserva quanto a questões específicas, a:

315.8.1. compartilhar com a Secretaria de Governo Digital do Ministério da Economia e com o Conselho Nacional de Justiça os dados das respostas individuais das organizações sob suas jurisdições ao questionário deste acompanhamento;

315.8.2. dar ampla divulgação às informações e aos produtos derivados deste acompanhamento, em especial à ficha-síntese e aos relatórios de *feedback* comparativos a serem elaborados, bem como a outros materiais (*e.g.* "Estratégia de Fiscalização do TCU em SegInfo e Privacidade de Dados 2022-2025", formulário *online* de autoavaliação e documentos técnicos visando a orientar os gestores quanto à implementação dos controles críticos e medidas de segurança avaliados em cada ciclo);

315.9. à luz dos arts. 23 e 24 da Lei 12.527/2011 (Lei de Acesso à Informação), classificar como reservados, por conterem informações consideradas imprescindíveis à segurança da sociedade ou do Estado:

315.9.1. as respostas individuais das organizações ao questionário deste acompanhamento;

315.9.2. o papel de trabalho da análise do incidente de segurança da informação/ataque *hacker* ocorrido no Ministério da Saúde em dezembro de 2021 (peça 854), a peça 811 e os itens não digitalizáveis dessas peças;

315.10. retornar os autos à Secretaria de Fiscalização de Tecnologia da Informação para dar continuidade ao presente acompanhamento.".

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 2/2/2022.

[ii] BRASIL. Tribunal de Contas da União (TCU). Boletim do TCU (BTCU) nº 21/2005. *Resolução - TCU nº 175, de 25 de maio de 2005*. Brasília: TCU, 2005. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/ato-normativo/*/TIPO%253A%2528Resolu%25C3%25A7%25C3%25A3o%2529%2520NUMATO%253A175%2520NUMANOATO%253A2005/score%2520desc/0>. Acesso em 2/2/2022.

[iii] BRASIL. Tribunal de Contas da União (TCU). *Manual de Acompanhamento*. Brasília: TCU, 2018. Disponível em: <https://portal.tcu.gov.br/manual-de-acompanhamento.htm>. Acesso em 2/2/2022.

[iv] 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 2/2/2022.

[v] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/031.436%252F2019-6/NUMEROSOMENTENUMEROS%253A3143620196/%2520>. Acesso em 2/2/2022.

[vi] Disponível em: <https://portal.tcu.gov.br/sistemas-criticos>. Acesso em Acesso em 2/2/2022.

[vii] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/001.873%252F2020-2/NUMEROSOMENTENUMEROS%253A187320202/%2520>. Acesso em 2/2/2022.

[viii] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/036.620%252F2020-3/NUMEROSOMENTENUMEROS%253A3662020203/%2520>. Acesso em 2/2/2022.

[ix] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/processo/039.606%252F2020-1/%2520/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/3/%2520>. Acesso em 2/2/2022.

[x] Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em 2/2/2022.

[xi] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/ato-normativo/*/TIPO:%22Portaria%22%20NUMATO:280%20NUMANOATO:2010/DTRELEVANCIA%20desc,NUMATO%20desc/0>. Acesso em 2/2/2022.

[xii] 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 2/2/2022.

[xiii] 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 2/2/2022.

[xiv] Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/autoavaliacao-de-controles>. Acesso em 2/2/2022.

[xv] Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em 2/2/2022.

[xvi] Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm>. Acesso em 2/2/2022.

[xvii] Disponível em: <https://pt.wikipedia.org/wiki/Ransomware>. Acesso em 2/2/2022.

[xviii] Disponível em: <https://tiinside.com.br/15/10/2020/brasileiros-sao-alvo-de-quase-metade-dos-ataques-de-ransomware-na-america-latina>. Acesso em 2/2/2022.

[xix] Disp. em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527>. Acesso em 2/2/2022.

[xx] Disponível em: <https://olhardigital.com.br/2020/12/31/noticias/ransomware-pode-se-tornar-um-problema-ainda-maior-em-2021>. Acesso em 2/2/2022.

[xxi] Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/latin-america-suffered-more-than-41-billion-cyberattack-attempts-in-2020>. Acesso em 2/2/2022.

[xxii] Disponível em: <https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2021/brasil-sofre-mais-16-2-bilhoes-tentativas-ataques-ciberneticos-na-primeira-metade-2021>. Acesso em 2/2/2022.

[xxiii] Disp. em: <https://www.kaspersky.com.br/blog/empresa-brasil-ransomware-pandemia/15527>. Acesso em 2/2/2022.

[xxiv] Disponível em: <https://www.kaspersky.com.br/blog/panorama-ciberameacas-brasil-2021-pesquisa/18020>. Acesso em 2/2/2022.

[xxv] Disponível em: <https://www.kaspersky.com.br/blog/hackers-ataques-cloud/18118>. Acesso em 2/2/2022.

[xxvi] UNITED KINGDOM. National Cyber Security Centre (NCSC). *Annual Review 2021: Making the UK the safest place to live and work online*. Londres: NCSC, 2021, 88p. Disponível em: <https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf>. Acesso em 2/2/2022.

[xxvii] Disponível em: <https://www.cisecurity.org/solarwinds>. Acesso em 2/2/2022.

[xxviii] Disponível em: <https://en.wikipedia.org/wiki/2021_Microsoft_Exchange_Server_data_breach>. Acesso em 2/2/2022.

[xxix] Disponível em: <https://inforchannel.com.br/2021/12/13/netskope-anuncia-tendencias-para-a-seguranca-cibernetica-em-2022>. Acesso em 2/2/2022.

[xxx] Disp. em: <https://www.techtarget.com/searchsecurity/feature/5-cybersecurity-predictions>. Acesso em 2/2/2022.

[xxxi] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9668.htm#anexo1>. Acesso em 2/2/2022.

[xxxii] Disponível. em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10363.htm>. Acesso em 2/2/2022.

[xxxiii] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/ctir-gov-em-numeros/visao-geral>. Acesso em 2/2/2022.

[xxxiv] Disponível em: <https://pt.wikipedia.org/wiki/Spamdexing>. Acesso em 2/2/2022.

[xxxv] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-06-2021>. Acesso em 2/2/2022.

[xxxvi] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-08-2021>. Acesso em 2/2/2022.

[xxxvii] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-03-2021>, <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-07-2021> e <https://www.gov.br/ctir/pt-br/assuntos/alertas-e-recomendacoes/alertas/2021/alerta-10-2021>. Acesso em 2/2/2022.

[xxxviii] Disponível em: <https://www.gov.br/ctir/pt-br/assuntos/noticias/2021/tendencias-de-ameacas-ciberneticas-as-infraestruturas-criticas>. Acesso em 2/2/2022.

[xxxix] Disponível em: <https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/index.cfm>. Acesso em 2/2/2022.

[xl] Disponível em: <https://www.cert.br/stats/incidentes>. Acesso em 2/2/2022.

[xli] Disponível em: <https://www.cert.br/stats/incidentes/2020-jan-dec/analise.html>. Acesso em 2/2/2022.

[xlii] Disp. em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2021-1/dezembro/nota-oficial>. Acesso em 2/2/2022.

[xliii] Disponível em: <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/12/atuacao-da-pf-no-ataque-hacker-ao-ministerio-da-saude>. Acesso em 2/2/2022.

[xliv] Disponível em: <https://www.cnnbrasil.com.br/nacional/site-do-ministerio-da-saude-sofre-ataque-hacker-durante-madrugada-e-sai-do-ar>. Acesso em 2/2/2022.

[xlv] Disp. em: <https://www.gov.br/saude/pt-br/assuntos/noticias/2021-1/dezembro/nota-a-imprensa>. Acesso em 2/2/2022.

[xlvi] Disponível em: <https://www.gov.br/gsi/pt-br/canais_atendimento/imprensa/nota-a-imprensa-13-dezembro.pdf>. Acesso em 2/2/2022.

[xlvii] Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2021/12/14/invasao-hacker-orgaos-do-governo.htm> e <https://noticias.r7.com/brasilia/ataque-de-hackers-derruba-sistemas-e-exclui-dados-da-pf-e-prf-20122021>. Acesso em 2/2/2022.

[xlviii] Disponível em: <https://datasus.saude.gov.br/datasus-restabelece-acesso-as-plataformas-do-ministerio-da-saude>. Acesso em 2/2/2022.

[xlix] Disponível em: <https://agenciabrasil.ebc.com.br/saude/noticia/2022-01/saude-sistemas-de-dados-serao-normalizados-ate-sexta>. Acesso em 2/2/2022.

[l] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/017.245%252F2017-6/NUMEROSOMENTENUMEROS%253A1724520176/%2520>. Acesso em 2/2/2022.

[li] Disponível em: <https://pesquisa.apps.tcu.gov.br/#/resultado/processo/011.574%252F2021-6/NUMEROSOMENTENUMEROS%253A1157420216/%2520>. Acesso em 2/2/2022.

[lii] International Telecommunication Union (ITU). *Global Cybersecurity Index (GCI) 2020*. Genebra: ITU Publications, 2021, 172p. Disp. em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf>. Acesso em 2/2/2022.

[liii] Disponível em: <https://www.in.gov.br/web/dou/-/emenda-constitucional-n-115-379516387>. Acesso em 2/2/2022.

[liv] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgpd>. Acesso em 2/2/2022.

[lv] BRASIL. Tribunal de Contas da União (TCU). *Acórdão 1.889/2020-TCU-Plenário*. Relator: Ministro Aroldo Cedraz. Brasília: TCU, 22/7/2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/NUMACORDAO%253A1889%2520ANOACORDAO%253A2020/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0>. Acesso em 2/2/2022.

[lvi] Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes>. Acesso em 2/2/2022.

[lvii] Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-aceita-como-membro-da-global-privacy-enforcement-network-gpen>. Acesso em 2/2/2022.

[lviii] Disp. em: <https://globalprivacyassembly.org/participation-in-the-assembly/list-of-observers>. Acesso em 2/2/2022.

[lix] Disponível em: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. Acesso em 2/2/2022.

[lx] Disponível em: <https://www.redipd.org/es/paises?nid=92>. Acesso em 2/2/2022.

[lxi] Disponível em: <https://www.oecd-ilibrary.org/sites/45a84b29-pt/index.html?itemId=/content/publication/45a84b29-pt>. Acesso em 2/2/2022.

[lxii] EUA. Cybersecurity & Infrastructure Security Agency (CISA). *CISA INSIGHTS - Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats*. 18/1/2022, 2p. Disponível em: <https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf>. Acesso em 2/2/2022.

[lxiii] Brasil. Tribunal de Contas da União. *Guia de boas práticas em contratação de soluções de tecnologia da informação: riscos e controles para o planejamento da contratação* / Tribunal de Contas da União. – Versão 1.0. – Brasília: TCU, 2012. 527 p. Disponível em: <https://portal.tcu.gov.br/biblioteca-digital/guia-de-boas-praticas-em-contratacao-de-solucoes-de-tecnologia-da-informacao-1-edicao.htm>. Acesso em 20/4/2022.

[lxiv] Brasil. Ministério do Planejamento, Desenvolvimento e Gestão. Secretaria de Tecnologia da Informação e Comunicação. *Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação*. 2017. 204 p. Disponível em: <https://www.gov.br/economia/pt-br/assuntos/noticias/planejamento/lancada-nova-versao-do-guia-de-boas-praticas-em-contratacao-de-solucoes-de-ti>. Acesso em 20/04/2022.

# VOTO

Em exame, fiscalização do tipo acompanhamento, realizada no período de 3/8/2021 a 9/3/2022, com vistas a avaliar a maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança da informação e segurança cibernética.

2. O acompanhamento foi realizado aplicando-se a metodologia CSA (*Control Self Assessment*) de autoavaliação de controles internos por meio da disponibilização de questionário eletrônico para preenchimento pelos gestores das organizações participantes. No TCU, a unidade técnica responsável pelos trabalhos foi a Secretaria de Fiscalização de TI (Sefti).

3. Registro que este trabalho integra o segundo eixo da estratégia que vem sendo adotada pelo TCU para realizar a fiscalização da segurança da informação e da segurança cibernética na administração federal. Tal estratégia está estruturada em quatro dimensões: mapeamento de situação; diagnóstico de situação; indução de boas práticas e cumprimento de normas; e acompanhamento de ações.

4. A segurança da informação (SegInfo) e a segurança cibernética (SegCiber) têm ao longo dos anos ganhado relevância nos cenários estratégicos institucionais e nacionais devido à crescente digitalização de entidades e da sociedade como um todo. Não é de hoje que informações, processos de negócio e ativos migraram para o mundo online carregando consigo uma série de riscos decorrentes de possível violação das regras de acesso e de proteção desses ativos.

5. Conforme relatou a unidade técnica, o Brasil segue nas primeiras posições dos rankings internacionais no que tange à perpetração de ataques cibernéticos. Segundo narrou, o Brasil ocupou a oitava posição do mundo em número de ataques a dispositivos da internet das coisas (IOT) no período de abril a junho de 2021 e o quinto lugar em ataques de sequestro de dados em meados de 2021. Ainda de acordo com informações da empresa Fortinet, que coleta e analisa incidentes em todo o mundo, em 2020 ocorreram 41 bilhões de tentativas de ataques cibernéticos na América Latina, sendo 8,4 bilhões no Brasil, número que, somente na primeira metade de 2021, subiu para 16,2 bilhões (Brasil).

6. A respeito das modalidades de ataques, os ataques do tipo *ransomware*, em que há criptografia de arquivos de dados e de infraestrutura e solicitação de resgates, continuam aumentando em função da crescente utilização de modelo de comercialização em que criminosos se concentram na obtenção e venda do acesso inicial às redes a serem atacadas. As campanhas de *phishing* – baseadas na indução de um comportamento de risco por parte de um usuário, como clicar em links maliciosos – continuam sendo o principal vetor de ataque.

7. Também se destacou no relatório os indicadores que apontam aumento na atividade de *botnets* (redes de computadores infectados e que podem ser controlados remotamente) para ataque a dispositivos IoT (internet das coisas), o que pode se agravar com a chegada da tecnologia 5G, com aumento no número de dispositivos conectados e na velocidade disponível.

8. No âmbito da administração pública, esse cenário é de extrema preocupação, conforme se observou no episódio do "apagão de dados" do Ministério da Saúde ocorrido em plena pandemia mundial da Covid-19[1], afetando de maneira central o monitoramento dos casos de Covid, tanto por instituições de saúde, quanto pelos órgãos de imprensa e pela população em geral.

9. Naquele caso, o Ministério da Saúde sofreu ataque cibernético no início do mês de dezembro que comprometeu diversos sistemas de informação, incluindo aqueles ligados ao programa nacional de imunização, à conectividade entre as unidades do SUS (ConecteSus) e à emissão de

[1] https://www.cnnbrasil.com.br/saude/apagao-de-dados-do-ministerio-da-saude-deixa-monitoramento-da-pandemia-a-deriva/

certificados de vacinação. Várias unidades da federação informaram problemas para atualizar dados referentes ao número de casos diários e óbitos causados pela pandemia devido à instabilidade durante a fase de recuperação dos sistemas.

10. Embora atuação individualizada no âmbito do MS não tenha feito parte do planejamento inicial de escopo da presente fiscalização, a Sefti realizou reuniões e diligências junto ao Ministério para apuração das causas do incidente e acompanhamento das soluções adotadas, questões que analiso, posteriormente, em seção destacada da presente decisão.

11. Cabe registro que, no âmbito da administração pública federal, compete ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o planejamento, a coordenação e supervisão das atividades de segurança da informação, incluída a segurança cibernética, a gestão de incidentes, entre outras atividades nesse contexto, conforme dispõe o Anexo I do Decreto 9.668/2019. Entre as estruturas voltadas para essa finalidade, está o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), que passou a incluir o termo "prevenção" em seu título a partir da publicação do Decreto 10.951/2022.

12. Também merece destaque a recente edição do Decreto 10.748/2021, que instituiu a Rede Federal de Gestão de Incidentes Cibernéticos (Regic), de participação obrigatória dos órgãos e entidades integrantes da administração direta, autárquica e fundacional, e voluntária por parte de empresas públicas e sociedades de economia mista. Por meio da coordenação do CTIR Gov, a Regic tem como objetivos: divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos; compartilhar alertas sobre ameaças e vulnerabilidades; promover a cooperação e celeridade na resposta a incidentes; entre outros.

13. Segundo cenário mapeado pelo CTIR Gov, destacaram-se, em 2021, alertas emitidos sobre vulnerabilidades em sistemas de autenticação de usuários, ações maliciosas em ambientes de nuvem e ataques de *ransomware* diversos. O CTIR Gov apontou também tendência de ameaças cibernéticas às infraestruturas críticas e aos sistemas de informação governamentais.

14. No plano normativo, como ações em curso, o relatório técnico registra que, em reuniões realizadas no início de 2022, o GSI informou estar revisando regramentos já publicados e emitindo novas normas, além de estar em elaboração a minuta de um projeto de lei para tratar da Política Nacional de Segurança Cibernética (PNSC), bem como dos Planos Nacionais de Segurança das Infraestruturas Críticas (Plansic) e de Gestão de Incidentes Cibernéticos (Plangic), bem assim dos correspondentes planos setoriais.

15. Diante do macrocenário internacional e nacional avaliado pela fiscalização, reforçado pela materialização de riscos que afetaram severamente o funcionamento não somente de sistemas, mas de serviços fundamentais da administração pública, ainda que existam ações em andamento por parte de várias organizações públicas, resta mais que evidente a relevância de se acompanhar com prioridade a presente matéria ao longo do exercício.

## II – HISTÓRICO DE ATUAÇÃO DO TCU

16. Na temática em questão, recordo que o TCU realizou levantamento que teve por foco a identificação de sistemas de informação críticos na administração pública e a realização de diagnóstico da capacidade do Tribunal de realizar fiscalização sobre esses sistemas (Ac. 1.889/2020-TCU-Plenário, Rel. Min. Aroldo Cedraz). Naquela ocasião, vários riscos de segurança foram considerados para se avaliar os sistemas mais relevantes para fins de acompanhamento, tais como riscos para vidas e saúde humanas, riscos às atividades finalísticas das organizações ou à segurança de infraestruturas críticas.

17. Já mais recentemente, tive a oportunidade de relatar dois trabalhos conexos com o presente acompanhamento: o levantamento de governança e gestão em segurança da informação e segurança cibernética na administração pública federal (Ac. 4.035/2020-TCU-Plenário) e a auditoria sobre a

efetividade dos procedimentos de backup e recuperação das organizações públicas (Ac. 1.109/2021-TCU-Plenário), mais conhecida como "auditoria do backup", cujo Acórdão autorizou a realização do presente acompanhamento.

18. No caso do primeiro levantamento, a decisão já relatava o aumento, de 16.355 em 2018 para 25.008 em 2019, no número de notificações de possíveis incidentes de segurança reportados ao Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov). Naquela época, destacaram-se pela quantidade os ataques de "abuso de sítio", ou seja, a desfiguração de páginas da internet, bem como os ataques de varredura ("scan") e os vazamentos de informações. Naquela ocasião, em dezembro de 2020, apontava-se que a ampliação do regime de trabalho remoto, reflexo da pandemia de Covid-19, havia ampliado o uso de serviços e softwares potencialmente vulneráveis, tais como redes privadas virtuais e aplicativos de videoconferência, ampliando os riscos de incidentes.

19. Posteriormente, no âmbito da auditoria de *backup*, restou uma vez mais demonstrada a fragilidade dos procedimentos adotados por muitas organizações federais, sendo que aproximadamente metade das organizações respondentes sequer tinham uma política de geração de cópias de segurança adotada. Além disso, das organizações que citaram contar com tal política, quase metade ainda não havia formalizado tal instrumento.

20. Tais trabalhos somam-se ainda a diversos outros que visam avaliar sistemas, políticas e processos digitais, tais como o acompanhamento da implementação da Identificação Civil Nacional, por mim relatada, e que resultou no Acórdão 1.453/2022-TCU-Plenário, o qual busca acompanhar os projetos e esforços no sentido de se oferecer uma solução nacional de identificação digital. Também nesse trabalho se destacou como premente a necessidade de se aperfeiçoar constantemente as práticas de segurança da informação para resguardar o sigilo de uma das bases de dados mais importantes para o país.

21. Portanto, a matéria que ora se aprecia é de vital importância, dada a crescente dependência de nossas instituições e serviços das tecnologias digitais. Com efeito, destaco que o presente acompanhamento está previsto para ser realizado em sete ciclos de execução, para avaliar até dezoito controles críticos de SegCiber, baseados no *framework* CIS, padrão internacional de boas práticas para adoção de controles de segurança, o qual passo a contextualizar nos parágrafos seguintes.

## III – DO *FRAMEWORK* E DA METODOLOGIA ADOTADOS

22. O *framework* CIS adotado como critério de referência para a condução deste trabalho está dividido em dezoito controles e 153 medidas de segurança, as quais estão divididas em três grupos de implementação: 56 básicas, 74 intermediárias e 23 avançadas. Os controles do *framework* estão descritos na tabela a seguir.

**Tabela 1 - Controles críticos de SegCiber preconizados pelo Center for Internet Security (CIS).**

| | |
|---|---|
| 1 | **Inventário e controle de ativos corporativos** |
| 2 | **Inventário e controle de ativos de software** |
| 3 | Proteção de dados |
| 4 | Configuração segura de ativos corporativos e de software |
| 5 | Gestão de contas |
| 6 | Gestão de controles de acesso |
| 7 | **Gestão contínua de vulnerabilidades** |
| 8 | Gestão de registros (*logs*) de auditoria |
| 9 | Proteções de *e-mail* e de navegador da *web* |
| 10 | Defesas contra *malware* |
| 11 | Recuperação de dados |
| 12 | Gestão de infraestrutura de rede |

| | |
|---|---|
| 13 | Monitoramento e defesa de rede |
| 14 | **Conscientização sobre segurança e treinamento de competências** |
| 15 | Gestão de provedores de serviço |
| 16 | Segurança de aplicações de software |
| 17 | **Gestão de respostas a incidentes** |
| 18 | Testes de invasão |

23. Nesse ciclo, foram avaliadas vinte medidas de segurança, todas do nível mais básico do *framework* de referência, e que fazem parte dos controles apontados em negrito na tabela anterior, quais sejam: Inventário e controle de ativos corporativos, Inventário e controle de ativos de software, Gestão contínua de vulnerabilidades, Conscientização sobre segurança e treinamento de competências, e Gestão de respostas a incidentes.

24. Vale lembrar que tais controles e suas respectivas medidas de segurança não fazem parte de metodologia estanque no cenário de normas e boas práticas de segurança da informação, estando presente também em inúmeros outros critérios normativos de referência, tais como instruções normativas do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e das normas brasileiras ABNT e ISO relativas à gestão de riscos e proteção à segurança das informações.

25. Para avaliação dos respectivos controles, a equipe de fiscalização lançou mão da realização de questionários eletrônicos, os quais eram preenchidos pelas próprias unidades gestoras mediante autoavaliação. De acordo com o relatório técnico, tal metodologia permite ampliar a abrangência do acompanhamento, mas contempla limitação no que diz respeito à qualidade das informações recebidas, uma vez que o instrumento é essencialmente declarativo. Nada obstante, em etapas futuras do acompanhamento os participantes serão instados a anexar evidências que suportem as principais respostas fornecidas.

26. Ainda assim, a unidade entende que, tendo em vista o caráter pedagógico do presente acompanhamento, tal limitação não desperta maiores preocupações. Outrossim, em casos específicos, podem ser realizadas auditorias pontuais para apuração de controles específicos ou de organizações que demandem maior atenção. Observo que, nesse mesmo sentido, apontam as considerações que farei oportunamente a respeito da situação observada no âmbito do Ministério da Saúde.

27. Feita essa breve contextualização, apresento a seguir a síntese dos principais achados, as respectivas conclusões e encaminhamentos acerca dos temas avaliados neste primeiro ciclo do acompanhamento.

## IV – ACHADOS IDENTIFICADOS PELA EQUIPE TÉCNICA

28. A partir dos resultados identificados pelos questionários aplicados junto aos entes jurisdicionados, o relatório técnico produzido consigna registros principais, os quais consistem em seis principais achados, cinco apontando falhas e problemas e um achado positivo, os quais estão resumidos nas seções seguintes.

29. O primeiro achado destacado consiste no diagnóstico de que ativos não autorizados que não estão sendo tratados pelos respectivos entes. São considerados como ativos corporativos de tecnologia da informação os equipamentos de usuários finais, tais como computadores portáveis e dispositivos móveis, dispositivos de rede e servidores, que se conectam fisicamente ou virtualmente à infraestrutura de TI.

30. Segundo avaliado, 88,1% das organizações possuem algum inventário de ativos corporativos, mas somente 44,3% (167 de 377) realizam algum tratamento sobre ativos não autorizados, efetivamente corrigindo-os ou removendo-os da rede. A presença de ativos não autorizados é um risco em potencial, pois invasores podem se valer da presença desse tipo de

hardware/software na organização para perpetrar ataques, ampliando-se o universo de possíveis riscos aos quais permanece exposta a organização.

31. O segundo achado relata a situação de que softwares não autorizados também não estão sendo tratados. De maneira semelhante ao primeiro achado, embora a maioria das organizações (71,4%) mantenha algum inventário de software, somente 55,2% (208 de 377) realizam algum tratamento de softwares não autorizados, como proceder sua desinstalação ou bloquear a sua execução. Ainda, os que procedem com a desinstalação, por exemplo, o fazem com frequência considerada insuficiente.

32. Por sua vez, o terceiro achado dispôs a respeito de deficiências nos processos de gestão e de correção de vulnerabilidades. Nesse caso, a maioria (57% - 215 de 377) das organizações relatou que ainda não estabeleceu um processo de gestão de vulnerabilidades. Tal controle é considerado crítico porque hoje em dia, grande parte dos ataques realizados por invasores diz respeito à pesquisa por vulnerabilidades que possam ser exploradas com sucesso. Por isso, para ser bem-sucedida, a defesa dos perímetros lógicos de segurança demanda acesso tempestivo a informações sobre vulnerabilidades em software e hardware, bem como às suas respectivas medidas de mitigação, de forma a corrigir antecipadamente as brechas que possam aproveitadas por potenciais invasores.

33. Nesse mesmo contexto há, entretanto, um relato positivo. O quarto registro do relatório indica que a gestão automatizada de correções de sistemas operacionais está sendo executada. Segundo o parecer da unidade especializada, 77,2% (291 de 377) das organizações afirmaram executar gestão automatizada de correções em sistemas operacionais, atuando para detectar e corrigir as vulnerabilidades no sistema operativo antes que possam ser exploradas pelos invasores.

34. O quinto apontamento realizado pela equipe técnica relata conscientização e treinamento deficientes no que tange aos riscos e às boas práticas de SegCiber. A carência de adoção desse tipo de prática já é conhecida há muito tempo pelo Tribunal de Contas da União, que vem apontando ao longo de uma série de trabalhos a necessidade de reforço no que tange ao aspecto humano da segurança das informações e da proteção cibernética.

35. Observou-se carência de treinamentos para identificar e notificar falta de atualizações nos ativos e sobre os riscos da transmissão de dados por meio de redes inseguras. Nota-se, ainda, que poucas organizações treinam seus colaboradores em técnicas de engenharia social ou em requisitos específicos de segurança antes de assumirem novos cargos, portanto, consoante relatou a fiscalização, as organizações de modo geral ainda estão em estágio inicial com relação à adoção desse controle.

36. Por fim, o sexto achado aponta que o processo de gestão de resposta a incidentes de segurança é deficiente. Apenas 47,5% (179 de 377) dos entes fiscalizados afirmaram manter um processo adequado para recebimento de notificação de incidentes. Cabe esclarecer que a gestão de resposta a incidentes é tida como medida essencial em um sistema de proteção organizacional, pois sabe-se que, em termos de segurança da informação e segurança cibernética, não existem sistemas ou organizações 100% seguros. Portanto, para que sistemas, serviços e processos possam ter maior resiliência e resistir a eventos de risco, contar com mecanismos eficientes de identificação e de resposta a incidentes é parte fundamental para o sucesso na proteção organizacional.

37. Nada obstante, apenas 65,8% das organizações designaram algum responsável por gerenciar o tratamento de incidentes de segurança, sendo que, entre as 248 organizações que disseram efetuar a designação, a grande maioria não revisa essa designação sequer anualmente. Diante do exposto, a avaliação apontou que a média e a mediana de notas das organizações com relação a esse quesito revelam que, de modo geral, ainda estamos em estágio inicial de capacidade com relação a esse controle.

## V – DOS INSTRUMENTOS DE ACOMPANHAMENTO E *FEEDBACK*

38. Diante do propósito pedagógico e informativo do presente trabalho, merece registro que, a

partir das informações coletadas mediante os questionários preenchidos pelas organizações fiscalizadas, foi construído um painel (*dashboard*) para permitir o acompanhamento efetivo da implementação dos controles críticos de SegCiber.

39. As informações presentes no painel podem ser visualizadas sob diferentes formatos e aspectos, permitindo inclusive análises e correlação com informações oriundas de outras fiscalizações. Devido ao sigilo nas informações tratadas, o acesso ao painel ficou restrito à equipe de auditores da UT.

40. Por outro lado, deve-se destacar que, a partir desses dados, foi possível realizar a construção de indicadores para cada um dos controles avaliados, de forma a permitir a avaliação individual de cada prática. Com isso, foi possível definir um indicador geral para sintetizar a maturidade geral da organização em SegCiber (iSegCiber). A metodologia de cálculo dos referidos indicadores consta do relatório técnico que fundamenta esta decisão.

41. Outro instrumento de caráter pedagógico adotado pelo presente trabalho foi o fornecimento de relatório de feedback individual na própria ferramenta de aplicação de questionário. Assim, ao final do preenchimento, cada gestor participante teve acesso imediato às suas notas nos indicadores relacionados a cada um dos controles verificados bem como à sua avaliação geral de maturidade (iSegCiber) e ao nível de SegCiber correspondente (Inexpressivo, Inicial, Intermediário ou Aprimorado).

42. Ainda a respeito das análises efetuadas, a fiscalização logrou identificar correlação positiva entre o indicador criado para aferir a maturidade da organização em gestão de SegInfo (iSegInfo) e aquele criado para medir a maturidade quanto à implementação de controles críticos de SegCiber (iSegCiber), em outras palavras, as fragilidades na adoção de controles críticos espelham uma falta de maturidade na gestão da segurança da informação.

43. Como possíveis causas dessas fragilidades, o relatório aponta carência de pessoal, de capacitação, de orçamento ou mesmo a falta de apoio da alta administração, o que se agrava diante da ausência de normativos que orientem e direcionem as unidades gestoras no que tange à implementação desses controles. Para fazer frente a esse cenário estão sendo dirigidas propostas de encaminhamento discutidas em seção própria deste Voto.

## VI – DO INCIDENTE CIBERNÉTICO NO MINISTÉRIO DA SAÚDE

44. Conforme relatado no início deste voto, os incidentes cibernéticos ocorridos no âmbito dos sistemas e serviços disponibilizados pelo Ministério da Saúde foram de extrema gravidade e se materializaram em momento de especial dificuldade, marcado pela maior crise de saúde pública vivida por nosso país em sua história recente.

45. Tão logo foram reportadas as primeiras informações a respeito do ataque sofrido, a unidade técnica procurou, no âmbito deste acompanhamento, obter informações junto aos gestores e responsáveis pela área técnica do Ministério da Saúde.

46. De acordo com as informações relatadas pela unidade técnica nos parágrafos 234 a 246 do relatório de fiscalização, o MS emitiu nota oficial informando sobre o incidente em 10/12/2021, afirmando que o evento deixou indisponíveis vários dos sistemas do Ministério, tais como o e-SUS Notifica, o Sistema de Informação do Programa Nacional de Imunização (SI-PNI) e o ConecteSUS, bem como as emissões do Certificado Nacional de Vacinação Covid-19 e da Carteira Nacional de Vacinação Digital. Segundo informações iniciais divulgadas pelo Departamento de Polícia Federal (DPF), o incidente envolveria o ambiente de nuvem pública do Ministério e teria comprometido sistemas de notificação de casos de covid, no âmbito do Programa Nacional de Imunização.

47. Em 12/12/2021, ou seja, dois dias após o incidente, o MS publicou nova nota informando que o processo para recuperação dos registros dos brasileiros vacinados contra a Covid-19 teria sido

finalizado sem perda de informações. No entanto, somente em 24/12/2021, o Departamento de Informática do SUS (Datasus) veio a informar que havia reestabelecido a disponibilidade do ConecteSUS Cidadão, permitindo a visualização dos dados vacinais e a emissão do Certificado Nacional de Vacinação Covid-19.

48. Entretanto, conforme apurou a Sefti, mais de um mês após o ataque, em 12/1/2022, foi noticiado na imprensa que o secretário executivo da pasta ministerial havia informado que sistemas ainda não disponíveis seriam normalizados até 14/1/2022.

49. Nada obstante, em reunião realizada com técnicos da pasta já em 25/2/2022, gestores do órgão relataram que os sistemas críticos haviam sido completamente restaurados, mas que estariam pendentes apenas algumas funcionalidades específicas de sistemas acessórios. Instados a apresentar uma listagem de quais seriam exatamente esses sistemas, até a data de elaboração da nota, o órgão não tinha fornecido à equipe as informações solicitadas. Ou seja, até a presente data, nem o TCU e nem tampouco a sociedade tem uma total dimensão do impacto ocorrido e do tempo consumido na restauração de sistemas e informações.

50. De todo modo, cabe-me destacar que a unidade técnica considerou que as ações realizadas pelo Ministério da Saúde para a resposta imediata e a recuperação dos sistemas afetados foram adequadas. Segundo relatou, há ainda indicativos de que os sistemas afetados estão operando em situação de normalidade, embora possam ocorrer algumas falhas de menor impacto. Salienta ainda que foram elaborados planos pelos gestores do órgão de modo a aprimorar os controles de segurança de modo a prevenir a ocorrência futura de incidentes semelhantes.

51. Em que pese os técnicos do MS terem adotado providências para promover a recuperação de dados e reestabelecer sistemas em cenário hostil e adverso, entendo que os danos diretos e indiretos causados pela indisponibilidade de serviços e informações necessários ao enfrentamento da pandemia sequer serão conhecidos em sua plenitude. Ao final do ano passado, vivemos verdadeiro apagão de dados, que prejudicaram ações a cargo dos organismos públicos de saúde, bem como prejudicaram o acompanhamento da evolução da pandemia por parte de toda a sociedade.

52. A despeito dos procedimentos adotados, o tratamento de caso concreto específico, de alta relevância, no âmbito de acompanhamento que tem caráter sistêmico, pedagógico e preventivo, não é a melhor solução. Dada a gravidade do ocorrido e a relevância da matéria para a população, penso que o assunto merece ser avaliado com maior profundidade, acompanhado e devidamente discutido por este Tribunal.

53. Caso assim não se procedesse, o exame de incidente de altíssima repercussão ficaria resumido a algumas reuniões preliminares e arquivado em papel de trabalho, não sendo devidamente examinado por essa Corte de Contas e alijando, por consequência, a sociedade de conhecer suas causas e os atos de gestão que estão sendo adotados para corrigir deficiências porventura existentes e para prevenir a ocorrência de situações semelhantes.

54. Por essas razões, proponho determinar a autuação de processo apartado para apuração das causas do incidente, avaliar a atuação das unidades gestoras frente ao ocorrido e das empresas contratadas para realizar a proteção e o provimento de infraestrutura ao órgão. Entendo que se deve analisar, ainda, de forma detida e peremptória, as providências adotadas para recuperar e corrigir as deficiências exploradas pelos invasores, submetendo o relatório e exame das providências adotadas ao Plenário deste Tribunal para apreciação.

55. Diante do exposto, sugiro ainda determinar que os TC 000.284/2022-0 e 000.372/2022-6, originalmente associados a estes autos, sejam apensados ao novo processo de acompanhamento a ser constituído.

## VII – PROPOSTAS FORMULADAS E COMENTÁRIOS DOS GESTORES

56. Retomando o escopo principal do presente acompanhamento, para fazer frente às diversas constatações de baixo grau de adoção de controles e de práticas tidos como básicos pelo *framework* adotado como referência, a unidade técnica propôs uma série de medidas destinadas às organizações fiscalizadas e submeteu o relatório preliminar do acompanhamento para comentários das respectivas unidades jurisdicionadas.

57. No que tange ao Ministério Público, destaca-se novamente manifestação do Conselho Nacional do Ministério Público (CNMP) no sentido de não reconhecer papel de Órgão Governante Superior (OGS), consoante decisão plenária adotada por aquele Conselho. Dessa forma, a unidade propõe dirigir os encaminhamentos formulados a cada um dos ramos do Ministério Público da União (MPU).

58. O Conselho Nacional de Justiça, por sua vez, fez solicitações que foram consideradas já atendidas ou que foram incorporadas pelo presente acompanhamento. Ainda, a unidade técnica salientou que a questão da contratação de soluções e serviços de TIC suscitada pelo CNJ não foi objeto da presente fiscalização.

59. No âmbito do poder executivo, o GSI se manifestou no sentido de que já definiu a estrutura mínima de gestão de segurança cibernética e os processos mínimos relativos à segurança cibernética que os órgãos devem possuir, entre eles o mapeamento de ativos, gestão de riscos, planejamento de contingência e continuidade de negócios, gestão de mudanças e avaliação de conformidade. Segundo afirmou, nesses documentos já se define o que deve ser feito e se recomenda a adoção das melhores práticas relativas ao assunto.

60. O órgão destaca que, em que pese reconhecer a abrangência do *framework* adotado como referência – o *CIS Controls V8* – existem outros frameworks e guias de boas práticas que são capazes de cumprir com as necessidades de segurança cibernética. A seu ver, a escolha do(s) modelo(s) deve caber a cada órgão ou entidade em função de sua capacidade operacional e maturidade para implementar os procedimentos de segurança necessários.

61. O GSI salienta que, como órgão normatizador, cabe ao GSI apenas determinar "o que deve ser feito'" ficando a cargo dos órgãos ou entes da APF definir a melhor forma de cumprir com a norma, evitando-se ingerência sobre as atividades dos entes sob sua supervisão. Pondera, assim, que a elaboração de guias de implementação caberia somente à Secretaria de Governo Digital do Ministério da Economia.

62. Por fim, o Gabinete de Segurança aponta que adotar o modelo preconizado pelo CIS implicaria custos adicionais para diversos órgãos e entidades que já adotaram outros *frameworks* de segurança e que seriam obrigados a fazer diversas adequações para manter conformidade com esse modelo.

63. A respeito das considerações do GSI, a Sefti aponta que as medidas de segurança adotadas na realização desse primeiro ciclo com base no *framework* CIS são consideradas básicas e são um indicativo de que as diversas normas do GSI/PR não estão sendo de fato observadas pelos órgãos e entidades das APF.

64. Ademais, reforça que tal framework foi adotado por ter caráter mais técnico e específico para segurança cibernética, mas que nada impede que, ao implementar seus controles de segurança, as organizações podem e devem utilizar outros frameworks de referência e não apenas o CIS. Além disso, destaca que tais controles formam um conjunto de ações de defesa de alta prioridade contra-ataques cibernéticos mais pervasivos e que, diante de um cenário de ameaças crescentes, são medidas consideradas imprescindíveis e urgentes para toda organização que precisa melhorar sua segurança cibernética.

65. Nesse sentido, alinho-me às conclusões esposadas pela unidade técnica. A adoção do *framework* como critério de referência para os questionamentos realizados pela fiscalização, muitos

em caráter inédito no âmbito de auditorias nessa matéria, não tem o condão e nem o propósito de substituir os normativos instituídos no âmbito do Poder Executivo, constituindo-se em referencial de boas práticas para proteção de organizações, serviços e informações. Como esclarecido pela unidade, há inúmeros guias e referenciais que podem ser adotados pelas organizações federais no âmbito de seu juízo discricionário de forma a cumprir os normativos e assegurar a devida proteção da segurança da informação e da segurança cibernética.

66. Aliás, tal discussão leva-me a refletir sobre a governança e a gestão da implementação dos controles de segurança por parte das organizações. Dada a profusão de guias, normas e frameworks de boas práticas no âmbito das práticas de segurança e proteção cibernética, penso que cabe aos OGS no âmbito do Poder Executivo orientar de forma ainda mais próxima a atuação das organizações federais, especialmente as menor maturidade e capacidade nessa área. Embora a discricionaridade na atuação da gestão seja indispensável, muitas organizações podem ter dificuldade na implementação de controles quando há grande distância entre as diretrizes estabelecidas pelos normativos e a implementação prática dos controles no dia a dia em seus processos.

67. Segundo a unidade técnica, esse contexto demonstra que permanece situação já apontada no levantamento realizado anteriormente pelo TCU (Ac. 4.035/2020-TCU-Plenário), em que a macroestrutura nacional responsável pela governança e gestão das questões de segurança da informação e segurança cibernética, embora atuante, não se mostrava adequada, dado o alcance limitado da atuação de seu principal órgão (GSI/PR), da regência do atual arcabouço normativo não alcançar a administração pública como um todo, mas tão somente o poder executivo, e considerando ainda que o papel orientador da SGD/ME restringe-se aos órgãos participantes do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo Federal.

68. Observo, portanto, que permanecem fragilidades estruturais no âmbito dos poderes da União no que diz respeito a questões sistêmicas, transversais, normativas e organizacionais para a efetiva proteção do espaço cibernético da administração pública, o que reforça a importância de se prosseguir o acompanhamento das ações voltadas ao fortalecimento da segurança em todos os seus aspectos.

69. Diante das constatações, acompanho, com ajustes parciais, as propostas da unidade técnica de recomendar ações visando o fortalecimento das adesões à Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do §4º, art. 7º, do Decreto 10.748/2021, bem como a manutenção de ações pedagógicas por parte da Secretaria de Governo Digital do Ministério da Economia.

70. Ainda, acompanho também as recomendações dirigidas aos demais poderes da República no sentido de implementarem controles críticos e medidas de segurança cibernética, bem como de, na ausência de normativos próprios, adotarem as práticas preconizadas pelos normativos editados no âmbito do Poder Executivo.

71. Por fim, cumpre-me destacar que a atuação na segurança da informação e na segurança cibernética é um desafio de todo o Estado brasileiro, incluindo o Tribunal de Contas da União e todos os demais órgãos de controle. Não há soluções mágicas e nem desafios simples quando se está a enfrentar as crescentes ameaças do espaço digital, as quais podem decorrer tanto de um invasor interno à própria organização, quanto podem ser oriundas de complexo e sofisticado aparato financiado por estados estrangeiros com interesses em nosso país.

72. Dessa forma, destaco que, o objetivo do presente trabalho é de atuar de forma propositiva e em consonância com as ações que já vem sendo desempenhadas pelos vários poderes da República e suas organizações. Com orçamentos apertados e múltiplas prioridades a cargo dos órgãos, sabe-se que os desafios do gestor público são numerosos. Ainda assim, há que se enfrentar esse novo contexto de ameaças digitais com a atenção que o assunto requer, dado que esse é o novo cenário em que os serviços públicos são prestados à sociedade. Como conclusão, espero que as recomendações e a

continuidade do presente trabalho, possam dar sua parcela de contribuição para o fortalecimento da segurança das informações públicas e do espaço cibernético brasileiro em prol do cidadão.

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

TCU, Sala das Sessões, em 3 de agosto de 2022.

Ministro VITAL DO RÊGO
Relator

ACÓRDÃO Nº 1768/2022 – TCU – Plenário

1. Processo TC 036.301/2021-3.
1.1. Apensos: 000.284/2022-0; 000.372/2022-6.
2. Grupo I – Classe de Assunto: V – Acompanhamento.
3. Interessados: Câmara dos Deputados (00.530.352/0001-59); Secretaria de Governo Digital do Ministério da Economia.
4. Entidades: vários.
5. Relator: Ministro Vital do Rêgo.
6. Representante do Ministério Público: não atuou.
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 acompanhamento com vistas a mapear a maturidade das organizações públicas federais quanto à implementação de controles críticos de segurança cibernética;

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

9.1. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, ao Gabinete de Segurança Institucional da Presidência da República que adote as seguintes providências:

9.1.1. comunicar aos órgãos e entidades da Administração Pública federal acerca da obrigatoriedade de suas adesões à Rede Federal de Gestão de Incidentes Cibernéticos em decorrência do § 1º do art. 1º do Decreto 10.748/2021;

9.1.2. promover e incentivar a adesão voluntária à Rede Federal de Gestão de Incidentes Cibernéticos por parte de empresas públicas e sociedades de economia mista federais, assim como de pessoas jurídicas de direito público interno dos Poderes Legislativo e Judiciário Federais (este último, por intermédio do Conselho Nacional de Justiça) e do Ministério Público da União, bem como a pessoas jurídicas de direito privado e a outras pessoas jurídicas de direito público (e.g. de entes federativos) consideradas relevantes para a formação dessa rede, consoante disposições constantes no §2º do art. 1º e §4º do art. 7º do Decreto 10.748/2021;

9.2. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, à Secretaria de Governo Digital do Ministério da Economia que, como órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) do Poder Executivo federal, avalie as deficiências apontadas neste ciclo do acompanhamento de forma a subsidiar suas ações normativas e pedagógicas, a fim de orientar os órgãos e entidades participantes desse sistema a implementarem com urgência controles críticos e medidas de segurança cibernética naquilo que lhes for aplicável, observando ainda as normas exaradas pelo Gabinete de Segurança Institucional da Presidência da República e boas práticas como as preconizadas pelo Center for Internet Security e pela norma técnica ABNT NBR ISO/IEC 27002:2013;

9.3. recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, ao Senado Federal, à Câmara dos Deputados, ao Tribunal de Contas da União, ao Supremo Tribunal Federal, ao Ministério Público Federal, ao Ministério Público Militar, ao Ministério Público do Trabalho e ao Ministério Público do Distrito Federal e Territórios que adotem as ações a seguir:

9.3.1. implementar com urgência controles críticos e medidas de segurança cibernética, de modo a tratar, em especial, as deficiências apontadas neste ciclo do acompanhamento, naquilo que lhes for aplicável, observando boas práticas como as preconizadas pelo Center for Internet Security e pela norma técnica ABNT NBR ISO/IEC 27002:2013;

9.3.2. adotar, na inexistência de normativo próprio tratando desses temas, as práticas previstas nos Decretos 9.637/2018 e 10.222/2020, que regem aspectos gerais relacionados à segurança da informação e à segurança cibernética no âmbito da Administração Pública federal, bem como as constantes das instruções normativas e de normas complementares editadas pelo Gabinete de Segurança Institucional da Presidência da República aplicáveis a esse respeito;

9.3.3. formalizar, junto ao Gabinete de Segurança Institucional da Presidência da República, ato de adesão à Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do § 4º do art. 7º do Decreto 10.748/2021;

9.4. recomendar ao Conselho Nacional de Justiça, com fundamento no art. 11 da Resolução - TCU 315/2020, que adote providências, tais como a edição de normativos e guias, assim como outras que entender aplicáveis, para orientar os tribunais sob sua supervisão administrativa com vistas à adoção das medidas constantes dos subitens 9.3.1 a 9.3.3;

9.5. dar ciência ao Ministério da Saúde, com fundamento no art. 9º, incisos I e II, da Resolução-TCU 315/2020, que a não designação de servidores para compor o comitê de segurança da informação ou estrutura equivalente do órgão ofende ao disposto no art. 15, inciso IV e § 1º, do Decreto 9.637/2018 e no art. 17 da Portaria 271/2017 desse ministério, que dispõe sobre a sua Política de Segurança da Informação e Comunicações, e constitui obstáculo para o atendimento às disposições do art. 8º da Instrução Normativa 5/2021 do Gabinete de Segurança Institucional da Presidência da República;

9.6. determinar à Secretaria de Fiscalização de TI que, com fundamento no art. 24, caput, c/c art. 24, parágrafo único, da Resolução-TCU 175/2005, tendo em vista o incidente cibernético que causou a interrupção de serviços essenciais à população no âmbito do Ministério da Saúde em dezembro de 2021, autue processo apartado de fiscalização para:

9.6.1. identificar as causas do incidente, bem como eventuais falhas de gestão e de controles que possam ter permitido ou agravado sua ocorrência, analisando-se, inclusive, apurações realizadas pelo Ministério da Saúde e demais órgãos;

9.6.2. avaliar as ações adotadas por empresas responsáveis pela prestação de serviços de infraestrutura e pela proteção das informações e dos serviços do Ministério da Saúde, no âmbito de suas obrigações contratuais;

9.6.3. acompanhar a adoção de medidas por parte do Ministério da Saúde para corrigir os problemas identificados, prevenir a ocorrência de novos incidentes e para reforçar a segurança das informações e a proteção cibernética dos serviços prestados no âmbito daquele órgão;

9.6.4. adotar outras providências que entender relevantes ao deslinde da questão.

9.7. determinar o desapensamento dos TC 000.284/2022-0 e 000.372/2022-6 destes autos e seu apensamento ao novo processo de acompanhamento a ser constituído em face do subitem anterior;

9.8. autorizar a Secretaria de Fiscalização de Tecnologia da Informação, a fim de alavancar a maturidade das organizações públicas federais relativamente à gestão de segurança cibernética e observada eventual necessidade de despersonificação e de reserva quanto a questões específicas a:

9.8.1. compartilhar com a Secretaria de Governo Digital do Ministério da Economia e com o Conselho Nacional de Justiça os dados das respostas individuais das organizações sob sua supervisão ao questionário deste acompanhamento;

9.8.2. em alinhamento com a Secretaria de Comunicação do TCU, dar ampla divulgação às informações e aos produtos derivados deste acompanhamento, em especial à ficha-síntese e aos relatórios de feedback comparativos a serem elaborados, bem como a outros materiais (e.g formulário online de autoavaliação e documentos técnicos visando a orientar os gestores quanto à implementação dos controles críticos e medidas de segurança avaliados em cada ciclo);

9.9. autorizar a Secretaria-Geral de Controle Externo, em articulação com a Secretaria de Fiscalização de Tecnologia da Informação e com Secretaria de Comunicação deste Tribunal, a realizar a divulgação da Estratégia de Fiscalização do TCU em SegInfo e Privacidade de Dados 2022-2025;

9.10. em atenção aos arts. 23 e 24 da Lei 12.527/2011 (Lei de Acesso à Informação), classificar como reservados, por conterem informações consideradas imprescindíveis à segurança da sociedade ou do Estado:

9.10.1. as respostas individuais das organizações ao questionário deste acompanhamento;

9.10.2. a análise do incidente de segurança da informação ocorrido no Ministério da Saúde em dezembro de 2021 (peça 854), a peça 811 e os itens não digitalizáveis dessas peças;

9.11. disponibilizar acesso ao Ministério da Saúde ao papel de trabalho contendo a análise do incidente de segurança da informação/ataque *hacker* ocorrido em dezembro de 2021 (peça 854), informando que se trata de documento classificado como reservado pelo TCU, para que tome conhecimento das conclusões da análise realizada pela Secretaria de Fiscalização de Tecnologia da Informação e das ações que foram identificadas como possíveis medidas complementares para auxiliar na mitigação de eventos futuros semelhantes e elevar a resiliência da organização;

9.12. determinar à Secretaria de Fiscalização de Tecnologia da Informação (Sefti) que efetue o monitoramento das recomendações contidas nos itens 9.1 a 9.4 constantes desta decisão;

9.13. encaminhar cópias eletrônicas deste acórdão, bem como do relatório e do voto que o fundamentam, ao GSI/PR; à SGD/ME; à Comissão de Ciência, Tecnologia, Inovação, Comunicação e Informática e à Presidência do Senado Federal; à Comissão de Ciência e Tecnologia, Comunicação e Informática e à Presidência da Câmara dos Deputados; ao TCU; ao STF; ao CNJ; ao MPF; ao MPT; ao MPM; e ao MPDFT;

9.14. notificar os demais órgãos fiscalizados acerca desta decisão;

9.15. retornar os autos à Secretaria de Fiscalização de Tecnologia da Informação para dar continuidade ao presente acompanhamento.

10. Ata n° 30/2022 – Plenário.
11. Data da Sessão: 3/8/2022 – Ordinária.
12. Código eletrônico para localização na página do TCU na Internet: AC-1768-30/22-P.
13. Especificação do quórum:
13.1. Ministros presentes: Bruno Dantas (na Presidência), Walton Alencar Rodrigues, Benjamin Zymler, Vital do Rêgo (Relator), Jorge Oliveira e Antonio Anastasia.
13.2. Ministros-Substitutos convocados: Marcos Bemquerer Costa e André Luís de Carvalho.
13.3. Ministro-Substituto presente: Weder de Oliveira.

(Assinado Eletronicamente)
BRUNO DANTAS
na Presidência

(Assinado Eletronicamente)
VITAL DO RÊGO
Relator

Fui presente:

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