TRIBUNAL DE CONTAS DA UNIÃO

Acompanhamento de controles críticos de segurança cibernética das organizações públicas federais

(TC 036.301/2021-3; Acórdão 1.768/2022-TCU-Plenário)

Relatório Individual de *Feedback*

FIOCRUZ
Fundação Oswaldo Cruz

Documento classificado como reservado por ser considerado imprescindível à segurança da sociedade ou do Estado (arts. 23 e 24 da Lei 12.527/2011 – LAI).

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

SUMÁRIO

1. Introdução 2
2. Indicadores de segurança cibernética 4
3. Seções do questionário 6
Controle 1 - Inventário e controle de ativos corporativos 6
Controle 2 - Inventário e controle de ativos de software 10
Controle 7 - Gestão contínua de vulnerabilidades 14
Controle 14 - Conscientização sobre segurança e treinamento de competências 20
Controle 17 - Gestão de respostas a incidentes 30
4. Boas práticas 35
Controle 1 - Inventário e controle de ativos corporativos 35
Controle 2 - Inventário e controle de ativos de software 35
Controle 7 - Gestão contínua de vulnerabilidades 35
Controle 14 - Conscientização sobre segurança e treinamento de competências 36
Controle 17 - Gestão de respostas a incidentes 36

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

1. Introdução

O processo de transformação digital (TD), 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 as organizações públicas 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*). O Brasil já é o oitavo do mundo em número de ataques a dispositivos da Internet das Coisas (*Internet of Things* – IoT) e o quinto em ataques de *ransomware* ("sequestro" de dados), que dispararam em 2020 e aumentaram 90% de 2020 para 2021.

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 estão expostas a riscos crescentes foi registrado no Acórdão 4.035/2020-TCU-Plenário (TC 001.873/2020-2, levantamento da governança e gestão de SegInfo e de SegCiber da APF; Rel. Min. Vital do Rêgo), cujo relatório sugeriu a "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023", que previa a realização deste acompanhamento.

Assim, autorizada por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de backup/restore dos órgãos e entidades da APF; Rel. Min. Vital do Rêgo), a Secretaria de Fiscalização de Tecnologia da Informação (Sefti), entre os dias 11/10 e 5/11/2021, utilizando a metodologia de autoavaliação de controles internos (*Control Self-Assessment* – CSA), aplicou um questionário online para obter dados e avaliar a adoção, pelas organizações públicas federais, de controles e medidas de segurança consideradas críticas no contexto da SegCiber.

O questionário foi elaborado com base na versão 8 do *framework* do *Center for Internet Security* (CIS), que prevê um total de dezoito controles críticos de SegCiber, subdivididos em 153 medidas de segurança: 56 básicas, 74 intermediárias e 23 avançadas. Essas medidas de segurança serão progressivamente avaliadas ao longo de sete ciclos de execução deste acompanhamento. Neste primeiro ciclo, foram avaliadas as medidas básicas dos 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; e

17) Gestão de respostas a incidentes.

Cabe ressaltar que as respostas constantes neste relatório são declaratórias e, portanto, de inteira responsabilidade dos gestores respondentes dos questionários aplicados no bojo deste acompanhamento.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Tendo em vista o caráter eminentemente didático do acompanhamento, foram gerados automaticamente relatórios como este, contendo as respostas individuais de cada organização participante, de modo que os gestores tenham subsídios para começarem a atuar para aperfeiçoar os controles e medidas de segurança envolvidos. Além destes relatórios individuais, também foram elaborados relatórios comparativos envolvendo as respostas de subgrupos de organizações com certa similaridade entre si.

Desse modo, a partir da ciência da sua própria realidade (com base no relatório individual) e da comparação dessa situação com aquela de um conjunto de organizações similares, espera-se conscientizar os gestores das áreas de SegInfo acerca dos riscos aos quais suas organizações estão sujeitas em virtude dos cada vez mais frequentes e sofisticados incidentes e ataques cibernéticos, contribuindo para o aumento gradativo da resiliência das organizações e o consequente esforço de transformação digital do País.

Destarte, o presente relatório apresenta, então, as respostas da organização: **Fundação Oswaldo Cruz**.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

2. Indicadores de segurança cibernética

De modo a consolidar os dados informados e oferecer um *feedback* referente às atividades de segurança cibernética, foram calculados indicadores 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 capacidade de suas atividades de gestão de segurança cibernética: Inexpressivo (iSegCiber <= 15), Inicial (15 < iSegCiber <= 50), Intermediário (50 < iSegCiber <= 80) e Aprimorado (iSegCiber > 80), resultando no indicador **nSegCiber**.

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 nota foi atribuída 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.

Nas questões do tipo B, a nota foi atribuída 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).

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 de SegCiber (**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 aos gestores, 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.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

A seguir são apresentados os valores dos indicadores calculados em função das respostas da organização (Tabela 1).

Tabela 1 - Indicadores de segurança cibernética

Nome	Valor
iControle1	28
iControle2	29
iControle7	0
iControle14	34
iControle17	78
iSegCiber	34
nSegCiber	Inicial

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

3. Seções do questionário

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 ela 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 mantêm ou gerenciam tais dados, de modo a aplicar-lhes controles de segurança adequados.

Referências úteis:
- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 1 (*Inventory and Control of Enterprise Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- *Information Technology Infrastructure Library* (ITIL) v3, *Service Transition*, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

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

1.1. Estabelecer e manter um inventário detalhado de ativos corporativos;

1.2. Tratar ativos não autorizados.

A seguir são apresentados os valores do indicador iControle1 e as notas das medidas de segurança calculados em função das respostas da organização (**Erro! Fonte de referência não encontrada.**).

Tabela 2 - iControle1 e medidas de segurança correspondentes

Nome	Valor
iControle1	28
Medida 1.1	55
Medida 1.2	0

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um inventário detalhado de ativos corporativos, com informações precisas, detalhadas e atualizadas sobre todos os ativos de hardware da organização que, potencialmente, armazenam, transmitem e/ou processam dados.

A seguir, são apresentadas as respostas à questão 1.1.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 1.1.2 (Tabela 3).

A subquestão 1.1.1.1 só era apresentada se a resposta à questão 1.1.1 fosse "Adota parcialmente"; a subquestão 1.1.1.2 só era apresentada se a resposta à questão 1.1.1 fosse "Adota em maior parte ou totalmente"; e a questão 1.1.2 só era apresentada se a resposta à questão 1.1.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

1.1.1. A organização estabelece e mantém um inventário detalhado de ativos corporativos?

a4) Adota parcialmente

1.1.1.1. Descreva as evidências da adoção parcial:

A instituição utiliza o software FusionInventory integrado ao GLPI para o inventário de ativos.

1.1.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

1.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o inventário de ativos (de hardware) existente na organização:

Tabela 3 - Questão 1.1.2

Subprática	Adota?
O inventário de ativos inclui dados dos equipamentos de usuários finais (incluindo computadores portáteis e dispositivos móveis)	Sim
O inventário de ativos inclui dados dos equipamentos servidores e dos dispositivos de rede da organização	Sim
O inventário de ativos inclui dados de dispositivos da Internet das Coisas (*Internet of Things* - IoT)	Não
O inventário inclui, para cada ativo, informações básicas (e.g. nome, endereços de rede [se estático] e de hardware [MAC *address*], proprietário/responsável, local [departamento, endereço]) e indicação se aquele ativo tem permissão/aprovação ou não para se conectar à rede da organização	Sim
A organização utiliza uma ferramenta de *Mobile Device Management* (MDM) para auxiliá-la a gerenciar os dispositivos móveis dos usuários finais	Não
O inventário inclui ativos conectados à infraestrutura da organização fisicamente, virtualmente e mesmo remotamente, incluindo aqueles em ambientes de nuvem (*cloud computing*)	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

O inventário inclui ativos conectados regularmente à infraestrutura de rede da organização, mesmo que não estejam sob seu controle	Não
As informações constantes no inventário de ativos são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Medida de segurança 1.2 - Tratar ativos não autorizados

Visão geral: ao identificar ativo não autorizado, a organização pode escolher remover o ativo da rede, negar que o ativo se conecte novamente na rede ou colocar o ativo em quarentena.

A seguir, são apresentadas as respostas à questão 1.2.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 1.2.2 (Tabela 4Tabela 3).

A subquestão 1.2.1.1 só era apresentada se a resposta à questão 1.2.1 fosse "Adota parcialmente"; a subquestão 1.2.1.2 só era apresentada se a resposta à questão 1.2.1 fosse "Adota em maior parte ou totalmente"; e a questão 1.2.2 só era apresentada se a resposta à questão 1.2.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

1.2.1. A organização trata ativos não autorizados?

a1) A organização não adota essa medida de segurança

1.2.1.1. Descreva as evidências da adoção parcial:

Não se aplica

1.2.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

1.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a forma como a organização lida com os ativos não autorizados:

Tabela 4 - Questão 1.2.2

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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.

Referências úteis:
- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 2 (*Inventory and Control of Software Assets*);
- ABNT NBR ISO/IEC 20000-2:2008, item 6.6.2 (Identificação e classificação dos ativos de informação);
- ABNT NBR ISO/IEC 27002:2013, item 8.1.1 (Inventário dos ativos);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.2 (Restrições quanto à instalação de software);
- *Information Technology Infrastructure Library* (ITIL) v3, *Service Transition*, item 4.3 (*Service Asset and Configuration Management* – SACM);
- Instrução Normativa GSI/PR 3/2021, Capítulo II (Mapeamento de ativos de informação).

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

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

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

Medida de segurança 2.3 - Tratar softwares não autorizados.

A seguir são apresentados os valores do indicador iControle2 e as notas das medidas de segurança calculados em função das respostas da organização (Tabela 5).

Tabela 5 - iControle2 e medidas de segurança correspondentes

Nome	Valor
iControle2	29
Medida 2.1	87
Medida 2.2	0
Medida 2.3	0

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um inventário detalhado de software, 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.

A seguir, são apresentadas as respostas à questão 2.1.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 2.1.2 (Tabela 6).

A subquestão 2.1.1.1 só era apresentada se a resposta à questão 2.1.1 fosse "Adota parcialmente"; a subquestão 2.1.1.2 só era apresentada se a resposta à questão 2.1.1 fosse "Adota em maior parte ou totalmente"; e a questão 2.1.2 só era apresentada se a resposta à questão 2.1.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

2.1.1. A organização estabelece e mantém um inventário detalhado de software?

a5) Adota em maior parte ou totalmente

2.1.1.1. Descreva as evidências da adoção parcial:

Não se aplica

2.1.1.2. Descreva as evidências da adoção em maior parte ou total:

A instituição utiliza o software FusionInventory integrado ao GLPI para o inventário de software.

2.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o inventário de software existente na organização:

Tabela 6 - Questão 2.1.2

Subprática	Adota?
O inventário inclui informações básicas (*e.g.* título do software, empresa responsável [editor/*publisher*], data da instalação, respectivo propósito de negócio)	Sim
Além das informações básicas, o inventário inclui informações adicionais sobre o software, tais como a URL (*Uniform Resource Locator*) 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.)	Não
As informações constantes no inventário de software são revisadas e atualizadas semestralmente (ou ainda mais frequentemente)	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: assegurar que apenas software atualmente suportado (previamente testado e homologado pelo setor de TI) seja designado como autorizado no inventário de software.

A seguir, são apresentadas as respostas à questão 2.2.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 2.2.2 (Tabela 7).

A subquestão 2.2.1.1 só era apresentada se a resposta à questão 2.2.1 fosse "Adota parcialmente"; a subquestão 2.2.1.2 só era apresentada se a resposta à questão 2.2.1 fosse "Adota em maior parte ou totalmente"; e a questão 2.2.2 só era apresentada se a resposta à questão 2.2.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

2.2.1. A organização assegura que apenas software atualmente suportado seja designado como autorizado no inventário de software?

a1) A organização não adota essa medida de segurança

2.2.1.1. Descreva as evidências da adoção parcial:

Não se aplica

2.2.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

2.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de autorização/homologação dos softwares na organização:

Tabela 7 - Questão 2.2.2

Subprática	Adota?
Usuários "comuns" são impossibilitados de instalar qualquer software não autorizado nas máquinas da organização	Não se aplica
Todo software autorizado (e, portanto, suportado) é testado e homologado previamente pelo setor de TI da organização	Não se aplica
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	Não se aplica
Todo e qualquer software não suportado para o qual não tenha sido documentada uma exceção é designado como "não autorizado"	Não se aplica
O inventário de software é revisado mensalmente (ou ainda mais frequentemente) para detectar softwares não suportados	Não se aplica

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Medida de segurança 2.3 - Tratar softwares não autorizados

Visão geral: tratar softwares não autorizados (softwares não suportados para os quais não tenha sido documentada uma exceção).

A seguir, são apresentadas as respostas à questão 2.3.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 2.3.2 (Tabela 8).

A subquestão 2.3.1.1 só era apresentada se a resposta à questão 2.3.1 fosse "Adota parcialmente"; a subquestão 2.3.1.2 só era apresentada se a resposta à questão 2.3.1 fosse "Adota em maior parte ou totalmente"; e a questão 2.3.2 só era apresentada se a resposta à questão 2.3.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

2.3.1. A organização trata softwares não autorizados?

a1) A organização não adota essa medida de segurança

2.3.1.1. Descreva as evidências da adoção parcial:

Não se aplica

2.3.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

2.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a forma como a organização lida com os softwares não autorizados:

Tabela 8 - Questão 2.3.2

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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.

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.

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.

Referências úteis:
- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 7 (*Continuous Vulnerability Management*);
- ABNT NBR ISO/IEC 27002:2013, item 12.6.1 (Gestão de vulnerabilidades técnicas).

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

<u>Medida de segurança 7.1 - Estabelecer e manter um processo de gestão de vulnerabilidades</u>

<u>Medida de segurança 7.2 - Estabelecer e manter um processo de correção de vulnerabilidades</u>

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

<u>Medida de segurança 7.4 - Executar a gestão automatizada de correções (*patches*) de aplicativos</u>

A seguir são apresentados os valores do indicador iControle7 e as notas das medidas de segurança calculados em função das respostas da organização (Tabela 9).

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Tabela 9 - iControle7 e medidas de segurança correspondentes

Nome	Valor
iControle7	0
Medida 7.1	0
Medida 7.2	0
Medida 7.3	0
Medida 7.4	0

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um 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.

A seguir, são apresentadas as respostas à questão 7.1.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 7.1.2 (Tabela 10).

A subquestão 7.1.1.1 só era apresentada se a resposta à questão 7.1.1 fosse "Adota parcialmente"; a subquestão 7.1.1.2 só era apresentada se a resposta à questão 7.1.1 fosse "Adota em maior parte ou totalmente"; e a questão 7.1.2 só era apresentada se a resposta à questão 7.1.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

7.1.1. A organização estabelece e mantém um processo de gestão de vulnerabilidades?

a1) A organização não adota essa medida de segurança

7.1.1.1. Descreva as evidências da adoção parcial:

Não se aplica

7.1.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

7.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de gestão de vulnerabilidades da organização:

Tabela 10 - Questão 7.1.2

Subprática	Adota?
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	Não se aplica
O processo de gestão de vulnerabilidades é revisado e atualizado anualmente (ou ainda mais frequentemente)	Não se aplica
O processo de gestão de vulnerabilidades define os diversos papéis e responsabilidades associados, incluindo, por exemplo, as atividades de monitoramento de vulnerabilidades, avaliação de risco de vulnerabilidades, aplicação de correções e acompanhamento dos ativos, bem como o desempenho da função de coordenação e a documentação associada a essas atividades	Não se aplica
O processo de gestão de vulnerabilidades está formalmente aprovado	Não se aplica
O processo de gestão de vulnerabilidades está documentado	Não se aplica

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um 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.

A seguir, são apresentadas as respostas à questão 7.2.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 7.2.2 (Tabela 11).

A subquestão 7.2.1.1 só era apresentada se a resposta à questão 7.2.1 fosse "Adota parcialmente"; a subquestão 7.2.1.2 só era apresentada se a resposta à questão 7.2.1 fosse "Adota em maior parte ou totalmente"; e a questão 7.2.2 só era apresentada se a resposta à questão 7.2.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

7.2.1. A organização estabelece e mantém um processo de correção de vulnerabilidades?

a1) A organização não adota essa medida de segurança

7.2.1.1. Descreva as evidências da adoção parcial:

Não se aplica

7.2.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

7.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de correção de vulnerabilidades da organização:

Tabela 11 - Questão 7.2.2

Subprática	Adota?
As vulnerabilidades e seus respectivos riscos são revisados mensalmente (ou ainda mais frequentemente)	Não se aplica
As correções das vulnerabilidades identificadas são priorizadas de acordo com os respectivos riscos (derivados de avaliações de probabilidade e impacto no negócio, por exemplo, para cada vulnerabilidade)	Não se aplica
O processo de correção de vulnerabilidades está formalmente aprovado	Não se aplica
O processo de correção de vulnerabilidades está documentado	Não se aplica

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: executar 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.

A seguir, são apresentadas as respostas à questão 7.3.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 7.3.2 (Tabela 12).

A subquestão 7.3.1.1 só era apresentada se a resposta à questão 7.3.1 fosse "Adota parcialmente"; a subquestão 7.3.1.2 só era apresentada se a resposta à questão 7.3.1 fosse "Adota em maior parte ou totalmente"; e a questão 7.3.2 só era apresentada se a resposta à questão 7.3.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

7.3.1. A organização executa a gestão automatizada da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos?

a1) A organização não adota essa medida de segurança

7.3.1.1. Descreva as evidências da adoção parcial:

Não se aplica

7.3.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

7.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de aplicação de correções (*patches*) nos sistemas operacionais da organização:

Tabela 12 - Questão 7.3.2

Subprática	Adota?
A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas aos sistemas operacionais utilizados, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados	Não se aplica
A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos	Não se aplica
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	Não se aplica
A verificação da necessidade de atualização/aplicação de correções (*patches*) nos sistemas operacionais ocorre mensalmente (ou ainda mais frequentemente)	Não se aplica

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: executar 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 aplicativos (programas) dos seus ativos.

A seguir, são apresentadas as respostas à questão 7.4.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 7.4.2 (Tabela 13).

A subquestão 7.4.1.1 só era apresentada se a resposta à questão 7.4.1 fosse "Adota parcialmente"; a subquestão 7.4.1.2 só era apresentada se a resposta à questão 7.4.1 fosse "Adota em maior parte ou totalmente"; e a questão 7.4.2 só era apresentada se a resposta à questão 7.4.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

7.4.1. A organização executa a gestão automatizada da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos?

a1) A organização não adota essa medida de segurança

7.4.1.1. Descreva as evidências da adoção parcial:

Não se aplica

7.4.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

7.4.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo de aplicação de correções (*patches*) nos aplicativos (programas) da organização:

Tabela 13 - Questão 7.4.2

Subprática	Adota?
A organização monitora constantemente fontes públicas e privadas de informações para identificar ameaças e vulnerabilidades relacionadas aos aplicativos (programas) utilizados, bem como a existência de correções (*patches*) e/ou de outras formas de mitigar os riscos associados	Não se aplica
A organização utiliza uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos	Não se aplica
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	Não se aplica
A verificação da necessidade de atualização/aplicação de correções (*patches*) nos aplicativos (programas) ocorre mensalmente (ou ainda mais frequentemente)	Não se aplica

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Controle 14 - Conscientização sobre segurança e treinamento de competências

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.

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.

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.

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.

Referências úteis:
- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 14 (*Security Awareness and Skills Training*);
- ABNT NBR ISO/IEC 27002:2013, item 7.2.2 (Conscientização, educação e treinamento em segurança da informação);
- Norma Complementar 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]).

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

<u>Medida de segurança 14.1 - Estabelecer e manter um programa de conscientização em segurança</u>

<u>Medida de segurança 14.2 - Treinar os colaboradores para reconhecerem ataques de engenharia social</u>

<u>Medida de segurança 14.3 - Treinar os colaboradores em melhores práticas de autenticação de usuários</u>

<u>Medida de segurança 14.4 - Treinar os colaboradores em melhores práticas de tratamento de dados</u>

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

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

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

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

A seguir são apresentados os valores do indicador iControle14 e as notas das medidas de segurança calculados em função das respostas da organização (Tabela 14).

Tabela 14 - iControle14 e medidas de segurança correspondentes

Nome	Valor
iControle14	34
Medida 14.1	30
Medida 14.2	46
Medida 14.3	42
Medida 14.4	35
Medida 14.5	42
Medida 14.6	35
Medida 14.7	0
Medida 14.8	45

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um 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.

A seguir, são apresentadas as respostas à questão 14.1.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.1.2 (Tabela 15).

A subquestão 14.1.1.1 só era apresentada se a resposta à questão 14.1.1 fosse "Adota parcialmente"; a subquestão 14.1.1.2 só era apresentada se a resposta à questão 14.1.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.1.2 só era apresentada se a resposta à questão 14.1.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.1.1. A organização estabelece e mantém um programa de conscientização em segurança?

a3) Adota em menor parte

14.1.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.1.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o programa de conscientização em segurança existente na organização:

Tabela 15 - Questão 14.1.2

Subprática	Adota?
O programa de conscientização em segurança está documentado	Não
O programa de conscientização em segurança está formalmente aprovado	Não
Os colaboradores recebem treinamento geral em segurança (como lidar com os ativos/dados corporativos de maneira segura) logo após sua contratação	Sim
Os colaboradores recebem treinamento geral em segurança anualmente (ou ainda mais frequentemente)	Não
O programa de conscientização em segurança considera os diferentes papéis desempenhados pelos colaboradores	Sim
Antes de assumirem novas posições na organização, os colaboradores recebem treinamento específico para os requisitos de segurança dos papéis a serem desempenhados	Não
O conteúdo do programa de conscientização em segurança é revisado e atualizado anualmente (ou ainda mais frequentemente)	Não
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	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.2.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.2.2 (Tabela 16).

A subquestão 14.2.1.1 só era apresentada se a resposta à questão 14.2.1 fosse "Adota parcialmente"; a subquestão 14.2.1.2 só era apresentada se a resposta à questão 14.2.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.2.2 só era apresentada se a resposta à questão 14.2.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.2.1. A organização treina seus colaboradores para reconhecerem ataques de engenharia social?

a4) Adota parcialmente

14.1.1.1. Descreva as evidências da adoção parcial:

Em seu último treinamento, realizado em maio/2021, foram abordados ataques de engenharia social, extorsão digital, spam, phishing, entre outros.

14.2.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em ataques de engenharia social recebido pelos colaboradores da organização:

Tabela 16 - Questão 14.2.2

Subprática	Adota?
O treinamento aborda ataques do tipo "carona" (*tailgating*)	Sim
O treinamento aborda ataques do tipo quiproquó (*quid pro quo*)	Sim
O treinamento aborda técnicas de "isca"	Não
O treinamento aborda técnicas de pretexto (*pre-texting*)	Não
O treinamento aborda ataques do tipo *phishing*	Não

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.3.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.3.2 (Tabela 17).

A subquestão 14.3.1.1 só era apresentada se a resposta à questão 14.3.1 fosse "Adota parcialmente"; a subquestão 14.3.1.2 só era apresentada se a resposta à questão 14.3.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.3.2 só era apresentada se a resposta à questão 14.3.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.3.1. A organização treina seus colaboradores em melhores práticas de autenticação de usuários?

a3) Adota em menor parte

14.3.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.3.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em práticas e autenticação de usuários recebido pelos colaboradores da organização:

Tabela 17 - Questão 14.3.2

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.4.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.4.2 (Tabela 18).

A subquestão 14.4.1.1 só era apresentada se a resposta à questão 14.4.1 fosse "Adota parcialmente"; a subquestão 14.4.1.2 só era apresentada se a resposta à questão 14.4.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.4.2 só era apresentada se a resposta à questão 14.4.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.4.1. A organização treina seus colaboradores em melhores práticas de tratamento de dados?

a3) Adota em menor parte

14.4.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.4.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.4.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em práticasde tratamento de dados recebido pelos colaboradores da organização:

Tabela 18 - Questão 14.4.2

Subprática	Adota?
O treinamento aborda a "política de mesa limpa e tela limpa"	Sim
A organização possui uma política de classificação da informação formalmente aprovada, cujo conteúdo faz parte do escopo do treinamento	Sim
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	Não
O treinamento aborda aspectos relacionados à deleção permanente de arquivos e dados (*data wiping*) e ao descarte seguro de mídias/equipamentos	Não

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.5.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.5.2 (Tabela 19).

A subquestão 14.5.1.1 só era apresentada se a resposta à questão 14.5.1 fosse "Adota parcialmente"; a subquestão 14.5.1.2 só era apresentada se a resposta à questão 14.5.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.5.2 só era apresentada se a resposta à questão 14.5.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.5.1. A organização treina seus colaboradores para evitarem exposição não intencional de dados?

a3) Adota em menor parte

14.5.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.5.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.5.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em exposição não intencional de dados recebido pelos colaboradores da organização:

Tabela 19 - Questão 14.5.2

Subprática	Adota?
O treinamento aborda aspectos relacionados à publicação de conteúdos da organização em aplicativos de mensageria e/ou em redes sociais	Sim
O treinamento aborda a conferência dos destinatários antes do envio de comunicações (*e.g. e-mails*) que contenham informações sensíveis	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)	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.6.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.6.2 (Tabela 20).

A subquestão 14.6.1.1 só era apresentada se a resposta à questão 14.6.1 fosse "Adota parcialmente"; a subquestão 14.6.1.2 só era apresentada se a resposta à questão 14.6.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.6.2 só era apresentada se a resposta à questão 14.6.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.6.1. A organização treina seus colaboradores para reconhecerem e notificarem incidentes de segurança?

a3) Adota em menor parte

14.6.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.6.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.6.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em reconhecimento e notificação de incidentes recebido pelos colaboradores da organização:

Tabela 20 - Questão 14.6.2

Subprática	Adota?
Além de capacitar os colaboradores a reconhecerem incidentes de segurança, o treinamento lhes ensina os canais e os meios apropriados para a respectiva notificação	Não
Além de ensinar os colaboradores a reconhecerem possíveis sinais da ocorrência de incidentes, o treinamento os capacita a identificarem (ou, pelo menos, terem alguma noção) o tipo, a extensão e a magnitude do problema	Não
O treinamento aborda os sinais precursores e indicadores da ocorrência de incidentes	Sim
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	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

A seguir, são apresentadas as respostas à questão 14.7.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.7.2 (Tabela 21).

A subquestão 14.7.1.1 só era apresentada se a resposta à questão 14.7.1 fosse "Adota parcialmente"; a subquestão 14.7.1.2 só era apresentada se a resposta à questão 14.7.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.7.2 só era apresentada se a resposta à questão 14.7.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.7.1. A organização treina seus colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos?

a1) A organização não adota essa medida de segurança

14.7.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.7.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.7.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento em identificação e notificação da falta de atualizações de segurança nos ativos corporativos recebido pelos colaboradores da organização:

Tabela 21 - Questão 14.7.2

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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*).

A seguir, são apresentadas as respostas à questão 14.8.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 14.8.2 (Tabela 22).

A subquestão 14.8.1.1 só era apresentada se a resposta à questão 14.8.1 fosse "Adota parcialmente"; a subquestão 14.8.1.2 só era apresentada se a resposta à questão 14.8.1 fosse "Adota em maior parte ou totalmente"; e a questão 14.8.2 só era apresentada se a resposta à questão 14.8.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

14.8.1. A organização treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras?

a3) Adota em menor parte

14.8.1.1. Descreva as evidências da adoção parcial:

Não se aplica

14.8.1.2. Descreva as evidências da adoção em maior parte ou total:

Não se aplica

14.8.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o treinamento sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras recebido pelos colaboradores da organização:

Tabela 22 - Questão 14.8.2

Subprática	Adota?
O treinamento aborda os riscos envolvidos na conexão de ativos corporativos a redes inseguras (*e.g.* captura de credenciais/senhas, comprometimento do ativo a partir da instalação de um *malware*)	Sim
O treinamento aborda os riscos envolvidos na transmissão de dados da organização por meio de redes inseguras (*e.g.* vazamento ou adulteração dos dados, exposição indevida de dados pessoais)	Sim
O treinamento aborda a evolução histórica dos protocolos de criptografia de redes *wi-fi* (WEP, WPA e WPA2), bem como suas diferenças em termos da segurança das respectivas conexões	Não
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	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Controle 17 - Gestão de respostas a incidentes

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.

Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes ocorrerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso acontecer. 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 prejuízos e recuperar dados e sistemas eventualmente corrompidos.

Referências úteis:
- *Framework* de controles críticos de SegCiber do CIS, versão 8, controle 17 (*Incident Response Management*);

- ABNT NBR ISO/IEC 27002:2013, item 16 (Gestão de incidentes de segurança da informação), em especial subitem 16.1.5 (Resposta aos incidentes de segurança da informação);

- Norma Complementar 5/IN01/DSIC/GSIPR (Criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR – nos órgãos e entidades da Administração Pública Federal [APF]);

- Norma Complementar 8/IN01/DSIC/GSIPR (Diretrizes para gerenciamento de incidentes em redes computacionais – gestão de ETIR – nos órgãos e entidades da Administração Pública Federal [APF]).

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

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

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

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

A seguir são apresentados os valores do indicador iControle17 e as notas das medidas de segurança calculados em função das respostas da organização (Tabela 23).

Tabela 23 - iControle17 e medidas de segurança correspondentes

Nome	Valor
iControle17	78
Medida 17.1	76
Medida 17.2	87
Medida 17.3	70

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: designar responsáveis por gerenciar o processo de tratamento de incidentes.

A seguir, são apresentadas as respostas à questão 17.1.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 17.1.2 (Tabela 24).

A subquestão 17.1.1.1 só era apresentada se a resposta à questão 17.1.1 fosse "Adota parcialmente"; a subquestão 17.1.1.2 só era apresentada se a resposta à questão 17.1.1 fosse "Adota em maior parte ou totalmente"; e a questão 17.1.2 só era apresentada se a resposta à questão 17.1.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

17.1.1. A organização designa responsáveis por gerenciar o processo de tratamento de incidentes?

a5) Adota em maior parte ou totalmente

17.1.1.1. Descreva as evidências da adoção parcial:

Não se aplica

17.1.1.2. Descreva as evidências da adoção em maior parte ou total:

A Fiocruz possui Modelo de Gestão de Incidente de Segurança da Informação (https://tic.fiocruz.br/sites/default/files/2020-05/Modelo%20de%20Gest%C3%A3o%20de%20Incidente%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20_0.pdf). A instituição também define uma Equipe de tratamento e resposta a incidentes em redes comptuacionais - ETIR (https://tic.fiocruz.br/sites/default/files/2020-05/Equipe%20de%20tratamento%20e%20resposta%20a%20incidentes%20em%20redes%20comptuacionais%20-%20ETIR%20.pdf), que designa o gestor de segurança da informação do órgão como o responsável.

17.1.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a designação de responsáveis por gerenciar o processo de tratamento de incidentes na organização:

Tabela 24 - Questão 17.1.2

Subprática	Adota?
A organização designa uma pessoa chave como responsável principal por gerenciar o processo de tratamento de incidentes (coordenar e documentar os esforços de resposta e recuperação de incidentes)	Sim
Além de designar um responsável principal, a organização designa ao menos mais um substituto (*backup*), sendo que este último colaborador não pode se afastar simultaneamente com o primeiro	Não
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	Sim

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

As designações dos responsáveis são revisadas anualmente (ou ainda mais frequentemente)	Não
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	Não

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter 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).

A seguir, são apresentadas as respostas à questão 17.2.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 17.2.2 (Tabela 25).

A subquestão 17.2.1.1 só era apresentada se a resposta à questão 17.2.1 fosse "Adota parcialmente"; a subquestão 17.2.1.2 só era apresentada se a resposta à questão 17.2.1 fosse "Adota em maior parte ou totalmente"; e a questão 17.2.2 só era apresentada se a resposta à questão 17.2.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

17.2.1. A organização estabelece e mantém informações de contato para reporte de incidentes de segurança?

a5) Adota em maior parte ou totalmente

17.2.1.1. Descreva as evidências da adoção parcial:

Não se aplica

17.2.1.2. Descreva as evidências da adoção em maior parte ou total:

Encontra-se definido no Modelo de Gestão de Incidente de Segurança da Informação (https://tic.fiocruz.br/sites/default/files/2020-05/Modelo%20de%20Gest%C3%A3o%20de%20Incidente%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%20_0.pdf) e na Equipe de tratamento e resposta a incidentes em redes comptuacionais - ETIR (https://tic.fiocruz.br/sites/default/files/2020-05/Equipe%20de%20tratamento%20e%20resposta%20a%20incidentes%20em%20redes%20comptuacionais%20-%20ETIR%20.pdf)

17.2.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam a relação contendo as informações de contato para reporte de incidentes de segurança mantida pela organização:

Tabela 25 - Questão 17.2.2

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter 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).

A seguir, são apresentadas as respostas à questão 17.3.1 e às suas respectivas subquestões, bem como às opções de subpráticas da questão 17.3.2 (Tabela 26).

A subquestão 17.3.1.1 só era apresentada se a resposta à questão 17.3.1 fosse "Adota parcialmente"; a subquestão 17.3.1.2 só era apresentada se a resposta à questão 17.3.1 fosse "Adota em maior parte ou totalmente"; e a questão 17.3.2 só era apresentada se a resposta à questão 17.3.1 fosse "Adota em menor parte", "Adota parcialmente" ou "Adota em maior parte ou totalmente".

17.3.1. A organização estabelece e mantém um processo para que os colaboradores possam notificar incidentes de segurança?

a5) Adota em maior parte ou totalmente

17.3.1.1. Descreva as evidências da adoção parcial:

Não se aplica

17.3.1.2. Descreva as evidências da adoção em maior parte ou total:

O processo se encontra mapeado.

17.3.2. Visando explicitar melhor o grau de adoção dessa medida de segurança, marque abaixo uma ou mais opções que majoritariamente caracterizam o processo para o recebimento de notificações de incidentes existente na organização:

Tabela 26 - Questão 17.3.2

Subprática	Adota?
Independentemente da revisão periódica, o processo é revisado sempre que a organização passa por uma mudança significativa que pode impactá-lo	Não
O processo é revisado anualmente (ou ainda mais frequentemente)	Sim
O processo é conhecido por e está à disposição de todos os colaboradores da organização	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	Não

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

4. Boas práticas

Controle 1 - Inventário e controle de ativos corporativos

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.

Controle 2 - Inventário e controle de ativos de software

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.

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.

Controle 7 - Gestão contínua de vulnerabilidades

Os processos de gestão e de correção de vulnerabilidades podem ser vistos como subfunções do processo de gestão de mudanças da organização e, portanto, aproveitar-se das 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*).

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).

Sobre aplicações de correções (*patches*), tendo em vista que os fornecedores estão sendo pressionados a liberarem esses pacotes 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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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). 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.

Controle 14 - Conscientização sobre segurança e treinamento de competências

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.

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.

Controle 17 - Gestão de respostas a incidentes

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.

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.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

TRIBUNAL DE CONTAS DA UNIÃO

Acompanhamento de controles críticos de segurança cibernética das organizações públicas federais (TC 036.301/2021-3)

Relatório Comparativo de *Feedback*

Subgrupo: Rod.I

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

SUMÁRIO

1. Introdução

2. Indicadores de segurança cibernética

3. Seções do questionário

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

1. Introdução

O processo de transformação digital, 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 as organizações públicas 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*). O Brasil já é o oitavo do mundo em número de ataques a dispositivos da Internet das Coisas (*Internet of Things* – IoT) e o quinto em ataques de *ransomware* ("sequestro" de dados), que dispararam em 2020 e aumentaram 90% de 2020 para 2021.

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 estão expostas a riscos crescentes foi registrado no Acórdão 4.035/2020-TCU-Plenário (TC 001.873/2020-2, levantamento da governança e gestão de SegInfo e de SegCiber da APF; Rel. Min. Vital do Rêgo), cujo relatório sugeriu a "Estratégia de Fiscalização do TCU em SegInfo e SegCiber 2020-2023" (https://portal.tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm), que previa a realização deste acompanhamento.

Assim, autorizada por meio do Acórdão 1.109/2021-TCU-Plenário (TC 036.620/2020-3, auditoria de *backup*/*restore* dos órgãos e entidades da APF; Rel. Min. Vital do Rêgo), a Secretaria de Fiscalização de Tecnologia da Informação (Sefti), entre os dias 11/10 e 5/11/2021, utilizando a metodologia de autoavaliação de controles internos (*Control Self-Assessment* – CSA), aplicou um questionário *online* para obter dados e avaliar a adoção, pelas organizações públicas federais, de controles e medidas de segurança consideradas críticas no contexto da SegCiber.

O questionário foi elaborado com base na versão 8 do *framework* do *Center for Internet Security* (CIS), que prevê um total de dezoito controles críticos de SegCiber, subdivididos em 153 medidas de segurança: 56 básicas, 74 intermediárias e 23 avançadas. Essas medidas de segurança serão progressivamente avaliadas ao longo de sete ciclos de execução deste acompanhamento. Neste primeiro ciclo, foram avaliadas as medidas básicas dos 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; e
17) Gestão de respostas a incidentes.

Nenhuma das 377 organizações participantes recebeu visita *in loco* e, portanto, <u>frisa-se que as respostas constantes neste relatório são de inteira responsabilidade dos gestores respondentes dos questionários aplicados no bojo deste acompanhamento</u>.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Tendo em vista o caráter eminentemente didático do acompanhamento, foram gerados automaticamente relatórios contendo as respostas individuais de cada organização participante, de modo que os gestores tenham subsídios para começarem a atuar para aperfeiçoar os controles e medidas de segurança envolvidos. Além dos relatórios individuais, também foram elaborados relatórios comparativos como este, envolvendo as respostas de subgrupos de organizações com certa similaridade entre si.

Desse modo, a partir da ciência da sua própria realidade (com base no relatório individual) e da comparação dessa situação com aquela de um conjunto de organizações similares, espera-se conscientizar os gestores das áreas de SegInfo acerca dos riscos aos quais suas organizações estão sujeitas em virtude dos cada vez mais frequentes e sofisticados incidentes e ataques cibernéticos, contribuindo para o aumento gradativo da resiliência das organizações e o consequente esforço de transformação digital do País.

Destarte, o presente relatório apresenta, então, o comparativo das respostas levando em consideração o subgrupo **Rod.I**, composto por 17 organizações com certa similaridade (Tabela 1).

Todos os gráficos foram extraídos de painel construído para essa finalidade no âmbito do acompanhamento.

Tabela 1 - Subgrupo Rod.I

Nome da Organização
Conselho Nacional de Desenvolvimento Científico e Tecnológico
Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
Fundação Alexandre de Gusmão
Fundação Biblioteca Nacional
Fundação Casa de Rui Barbosa
Fundação Cultural Palmares
Fundação Escola Nacional de Administração Pública
Fundação Habitacional do Exército
Fundação Instituto Brasileiro de Geografia e Estatística
Fundação Instituto De Pesquisa Econômica Aplicada
Fundação Joaquim Nabuco
Fundação Jorge Duprat Figueiredo de Segurança e Medicina do Trabalho
Fundação Nacional de Artes
Fundação Nacional de Saúde
Fundação Nacional do Índio
Fundação Osório
Fundação Oswaldo Cruz

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

2. Indicadores de segurança cibernética

De modo a consolidar os dados informados e oferecer um *feedback* referente às atividades de segurança cibernética, foram calculados indicadores 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 capacidade de suas atividades de gestão de segurança cibernética: Inexpressivo (iSegCiber <= 15), Inicial (15 < iSegCiber <= 50), Intermediário (50 < iSegCiber <= 80) e Aprimorado (iSegCiber > 80), resultando no indicador **nSegCiber**.

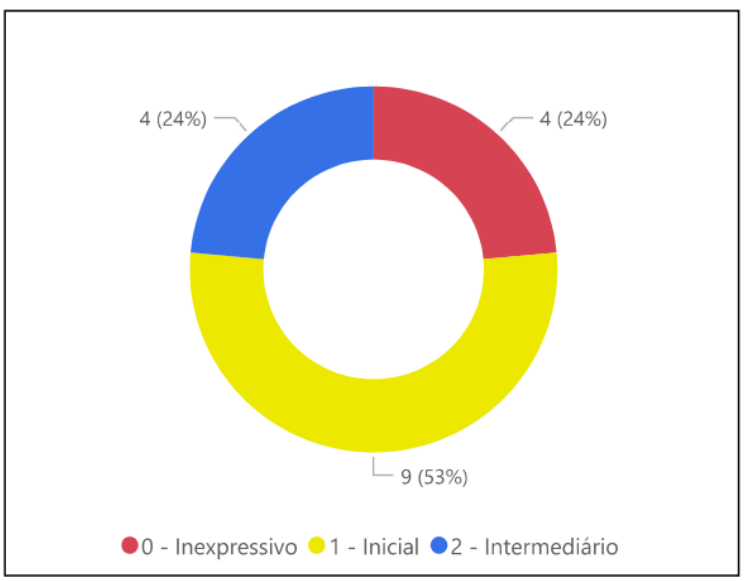

Figura 1 - Distribuição distribuição das organizações de acordo com o indicador **nSegCiber**

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 nota foi atribuída 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.

Nas questões do tipo B, a nota foi atribuída 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).

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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 de SegCiber **(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* 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.

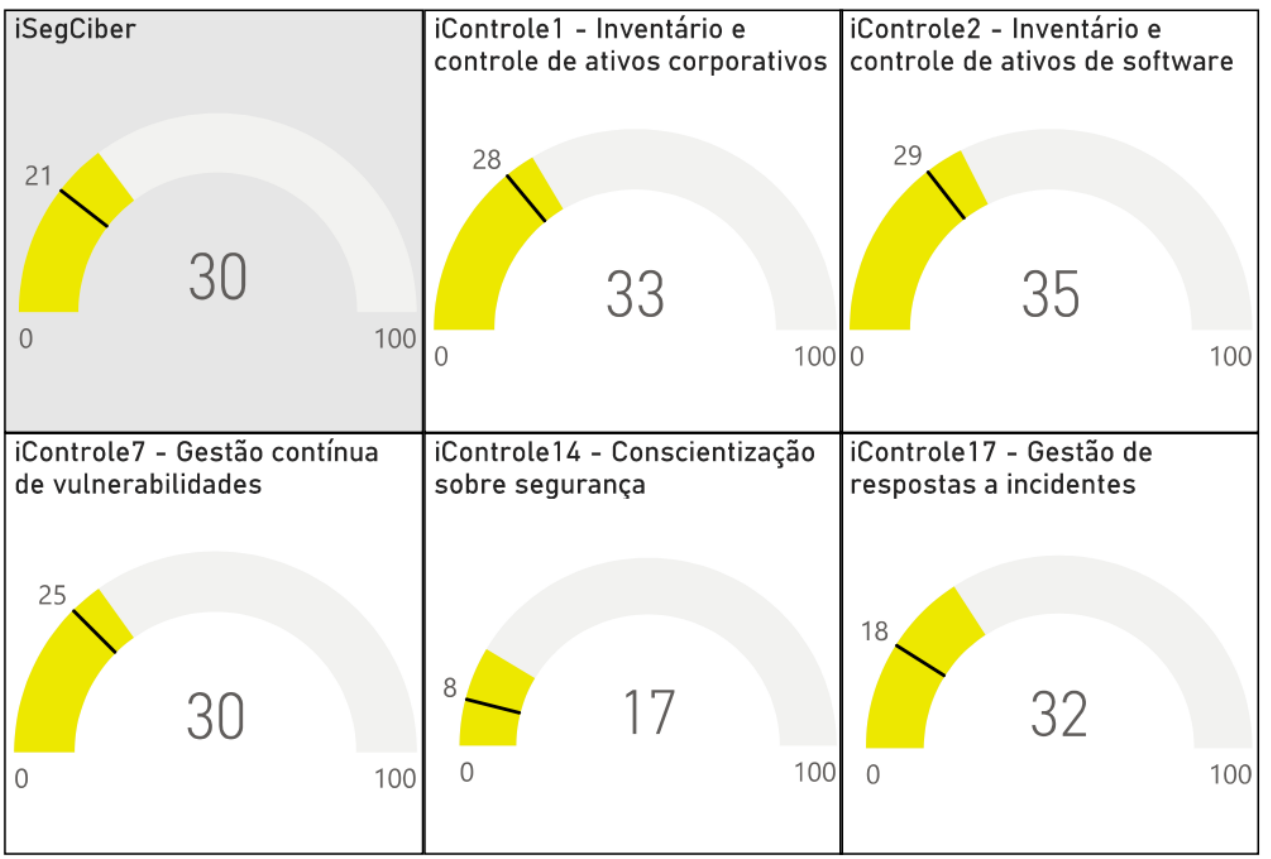

Figura 2 - iSegCiber, **iControle1**, **iControle2**, **iControle7**, **iControle14** e **iControle17**
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

3. Seções do questionário

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 ela 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 mantêm 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. Estabelecer e manter um inventário detalhado de ativos corporativos;
1.2. Tratar ativos não autorizados.

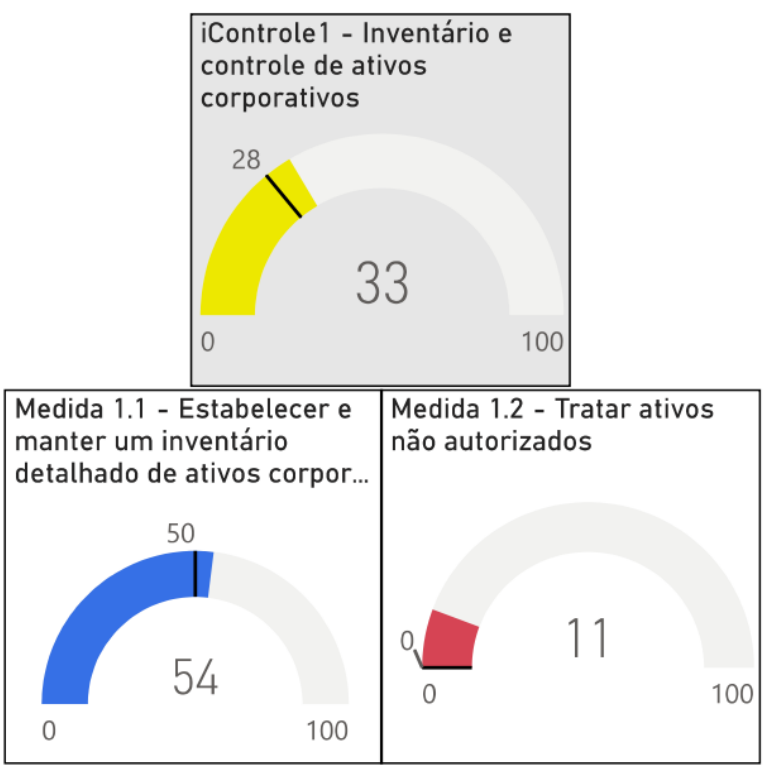

Figura 3 - iControle1 e medidas de segurança correspondentes
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um inventário detalhado de ativos corporativos, com informações precisas, detalhadas e atualizadas sobre todos os ativos de hardware da organização que, potencialmente, armazenam, transmitem e/ou processam dados.

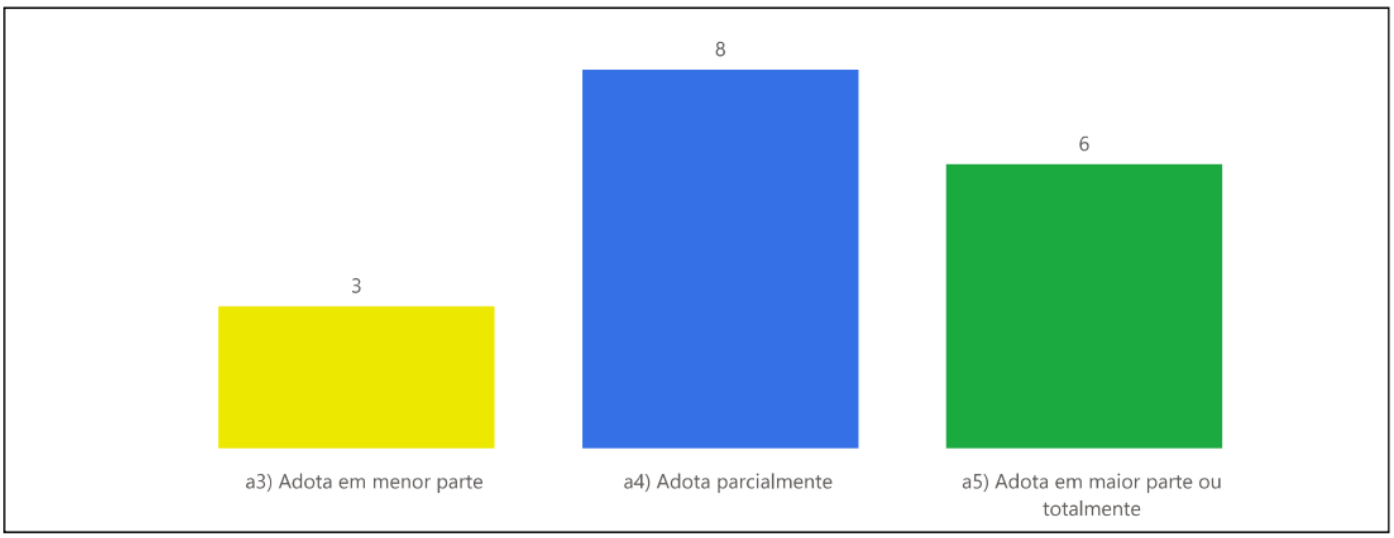

Figura 4 - Distribuição das respostas à **Questão 1.1.1** -
A organização estabelece e mantém um inventário detalhado de ativos corporativos?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Medida de segurança 1.2 - Tratar ativos não autorizados

Visão geral: ao identificar ativo não autorizado, a organização pode escolher remover o ativo da rede, negar que o ativo se conecte novamente na rede ou colocar o ativo em quarentena.

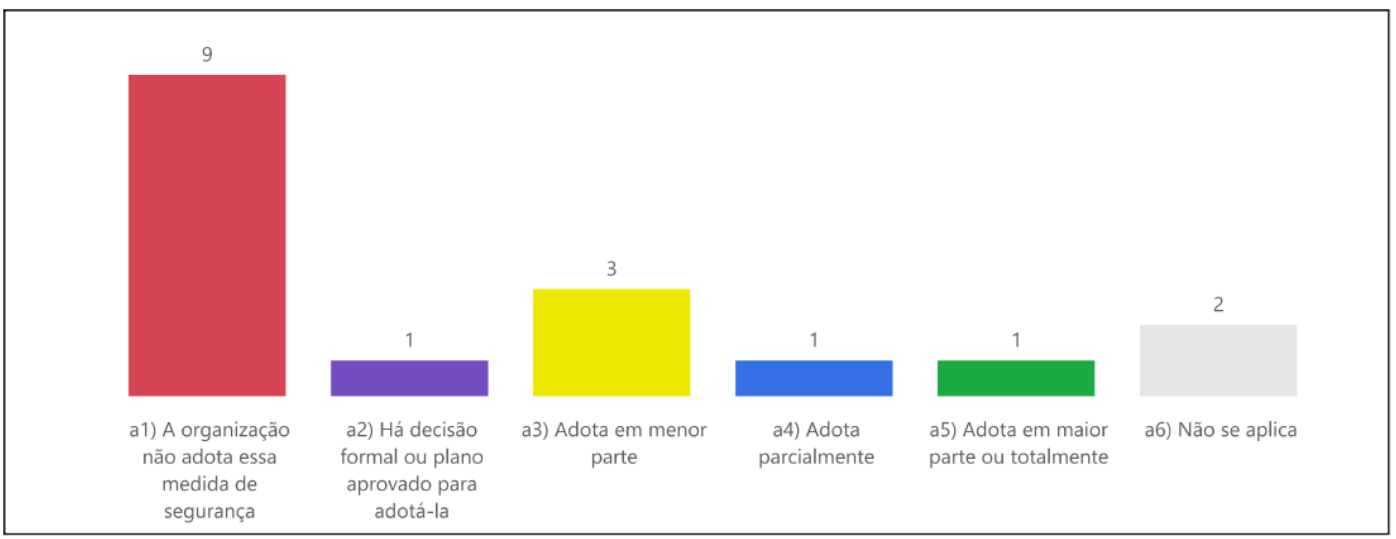

Figura 5 - Distribuição das respostas à **Questão 1.2.1** -
A organização trata ativos não autorizados?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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. Estabelecer e manter um inventário de software;
2.2. Assegurar que o software autorizado seja atualmente suportado;
2.3. Tratar softwares não autorizados.

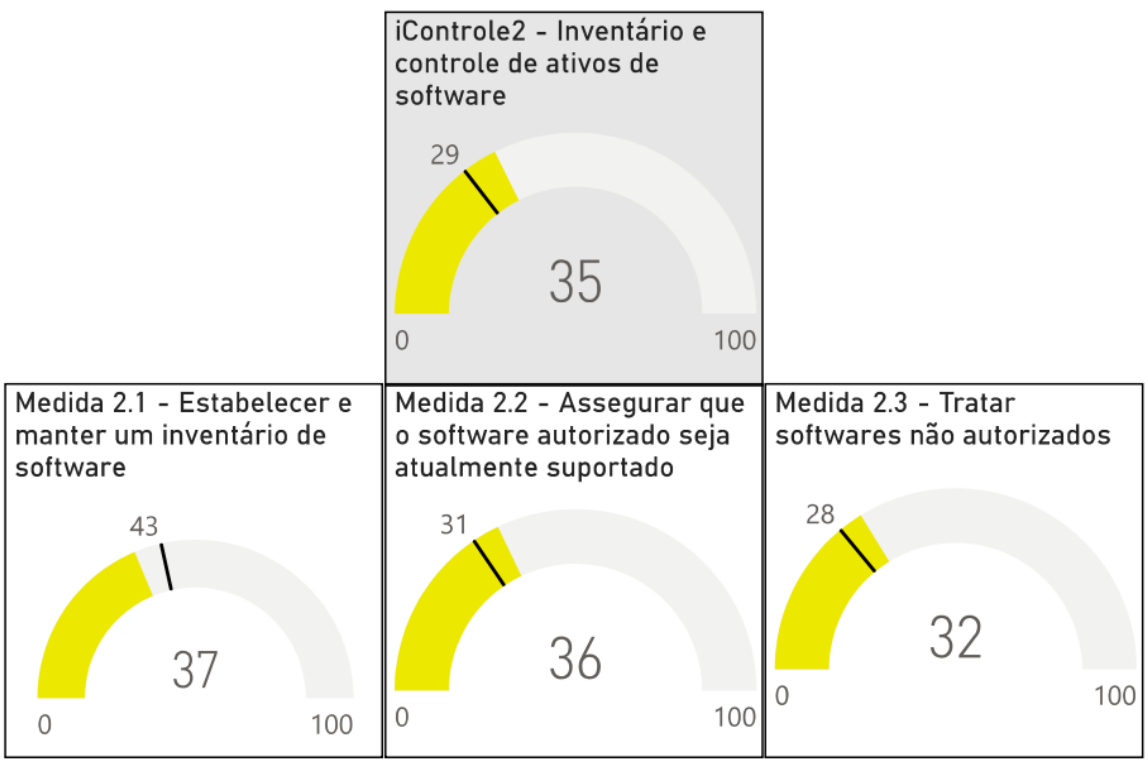

Figura 6 - iControle2 e medidas de segurança correspondentes
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um inventário detalhado de software, 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.

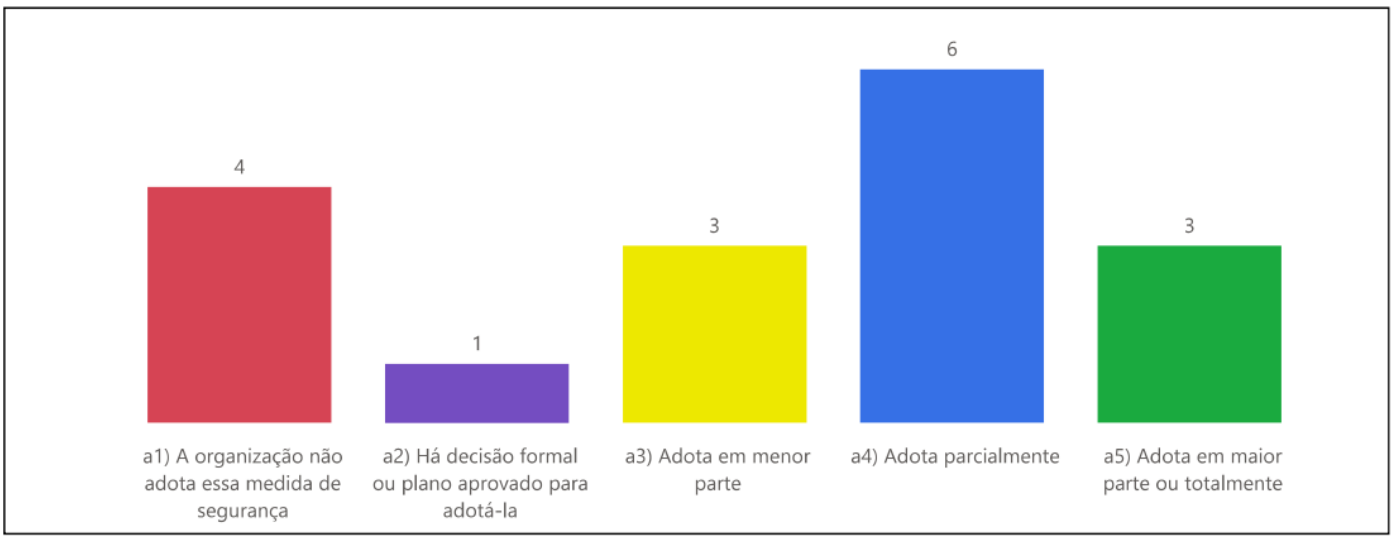

Figura 7 - Distribuição das respostas à **Questão 2.1.1** -
A organização estabelece e mantém um inventário detalhado de software?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: assegurar que apenas software atualmente suportado (previamente testado e homologado pelo setor de TI) seja designado como autorizado no inventário de software.

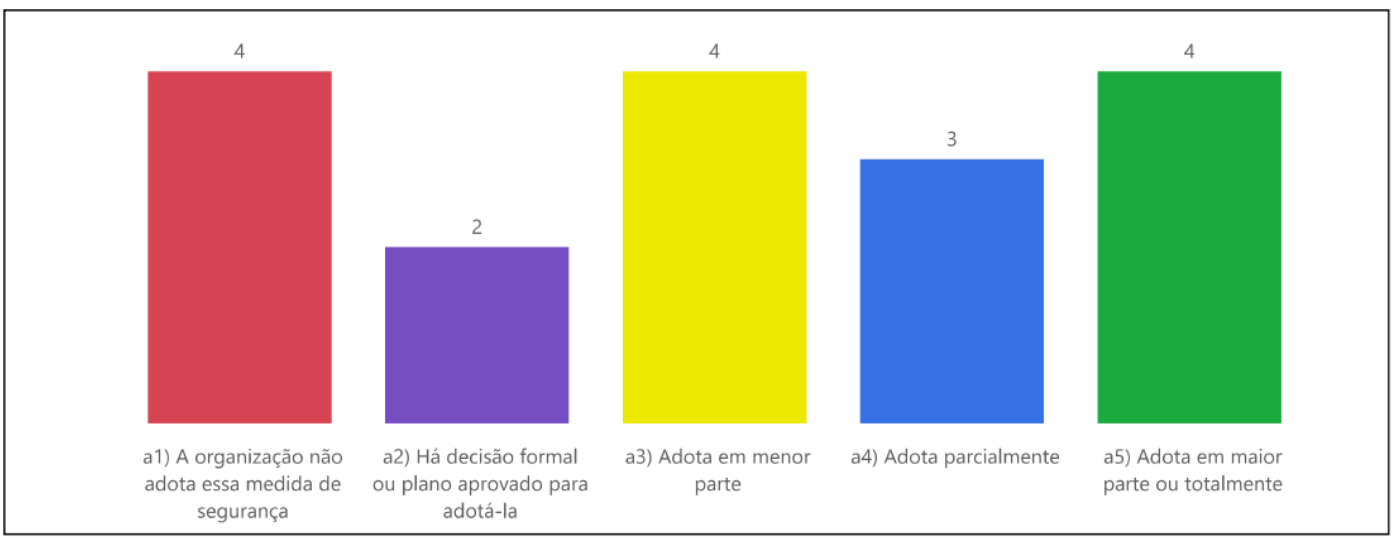

Figura 8 - Distribuição das respostas à **Questão 2.2.1** -
A organização assegura que apenas software atualmente suportado seja designado como autorizado no inventário de software?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Medida de segurança 2.3 - Tratar softwares não autorizados

Visão geral: tratar softwares não autorizados (softwares não suportados para os quais não tenha sido documentada uma exceção).

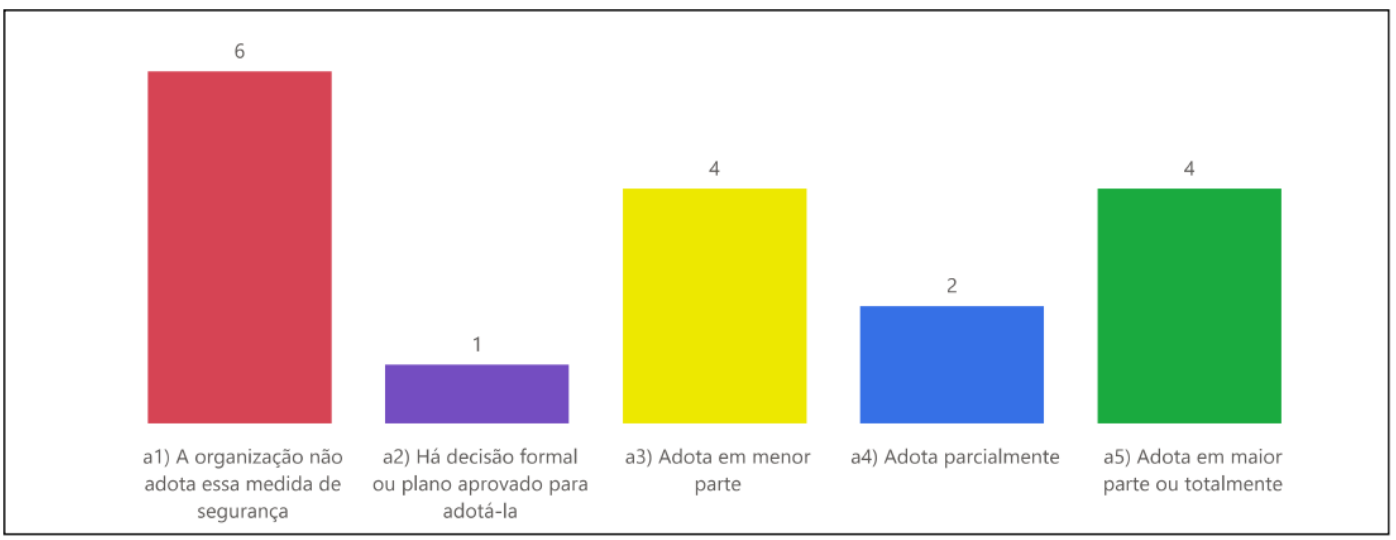

Figura 9 - Distribuição das respostas à **Questão 2.3.1** -
A organização trata softwares não autorizados?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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.

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.

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.

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

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.

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

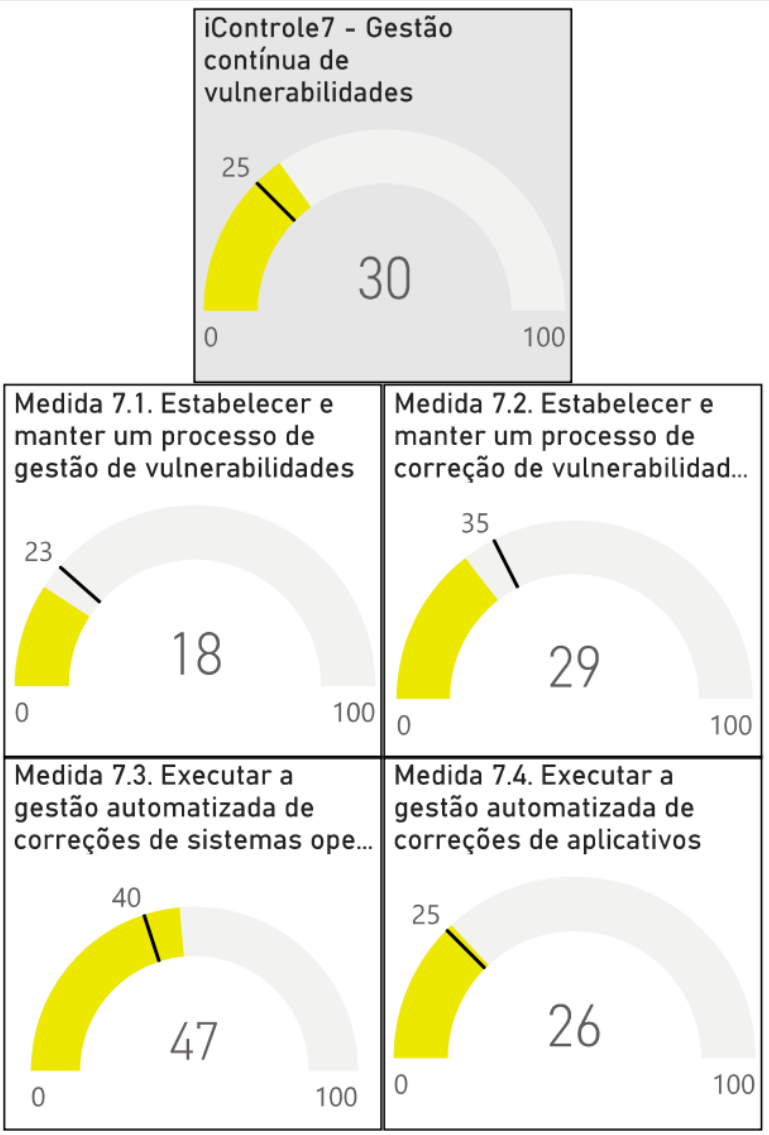

Figura 10 - iControle7 e medidas de segurança correspondentes
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um 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.

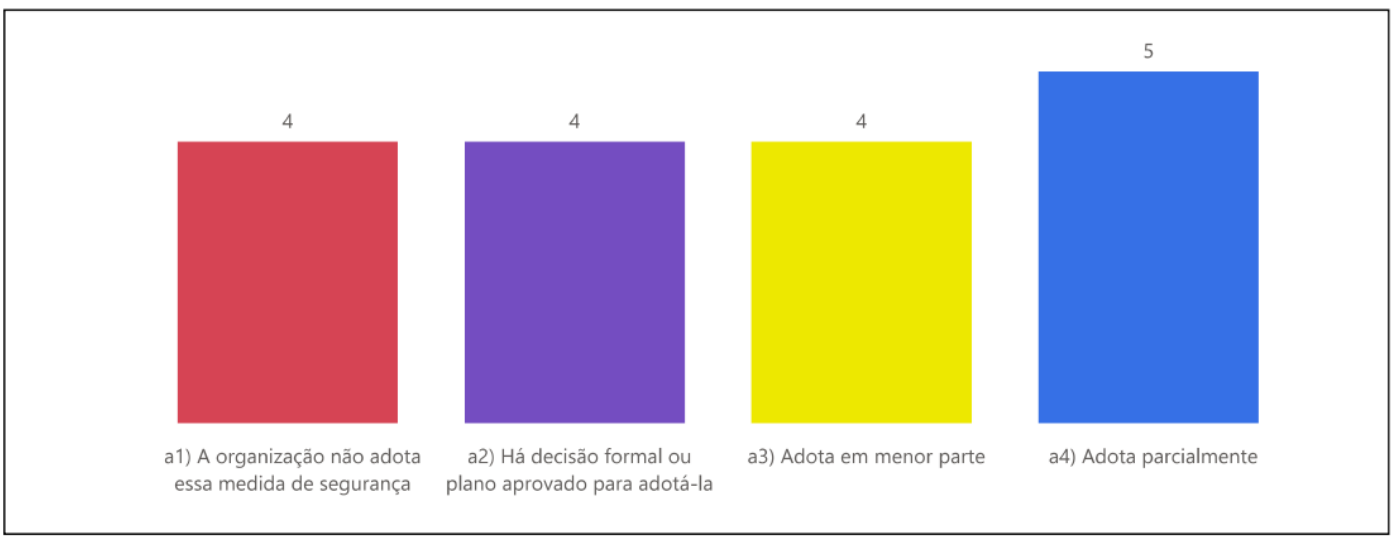

Figura 11 - Distribuição das respostas à **Questão 7.1.1** -
A organização estabelece e mantém um processo de gestão de vulnerabilidades?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter um 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.

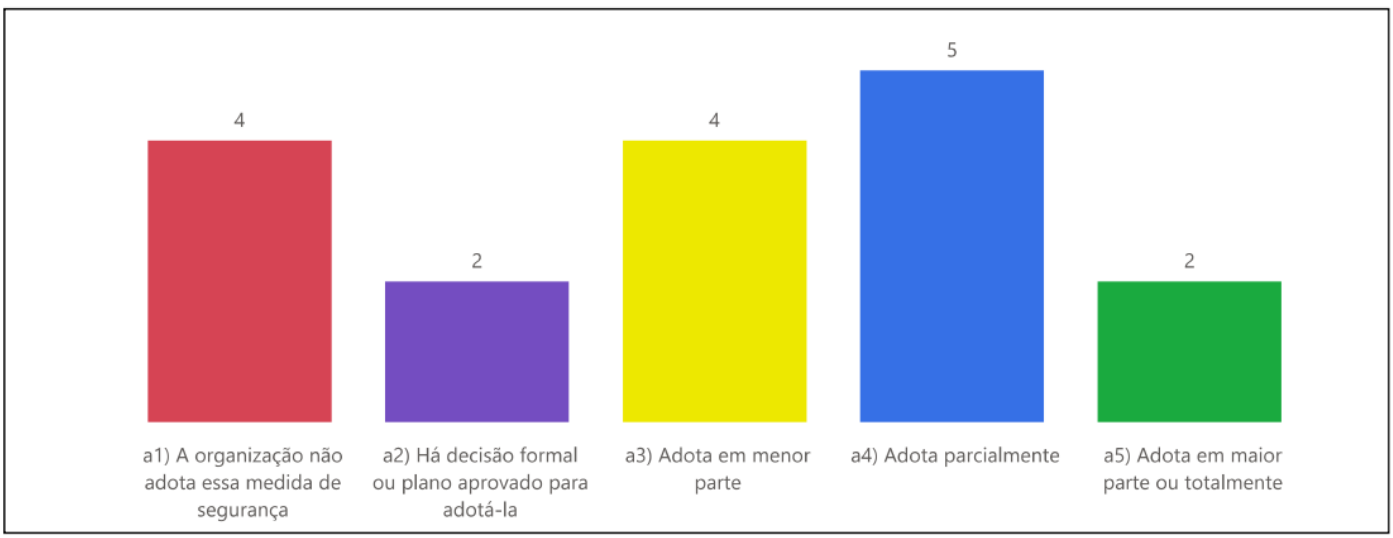

Figura 12 - Distribuição das respostas à **Questão 7.2.1** -
A organização estabelece e mantém um processo de correção de vulnerabilidades?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: executar 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.

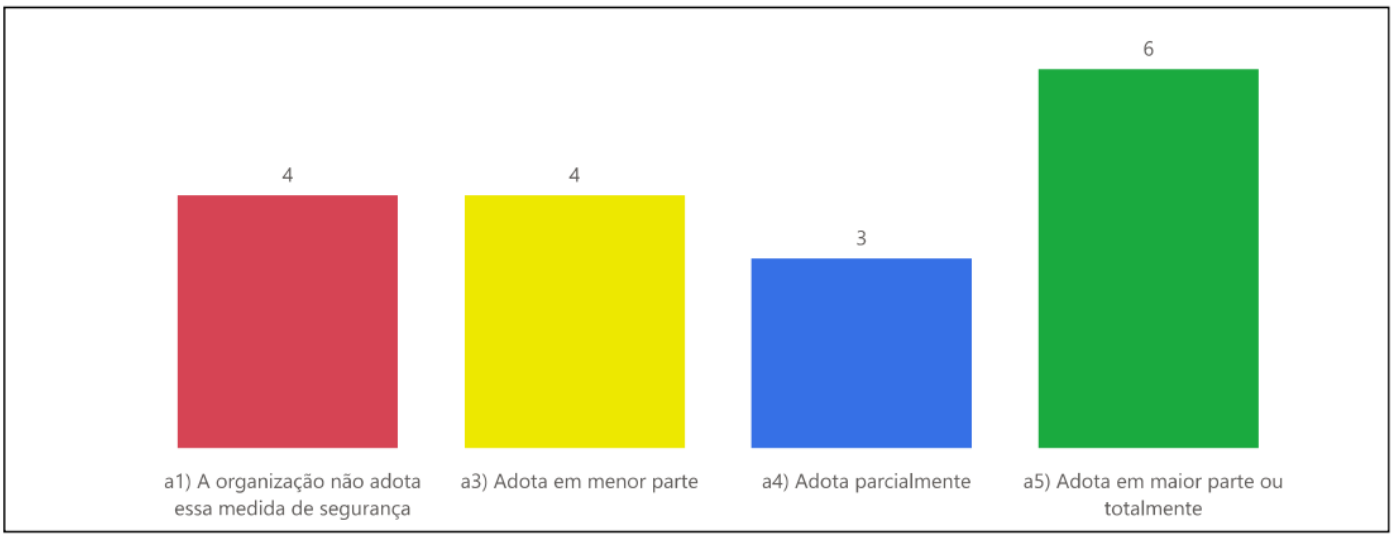

Figura 13 - Distribuição das respostas à **Questão 7.3.1** -
A organização executa a gestão automatizada da aplicação de correções (*patches*) nos sistemas operacionais dos seus ativos?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: executar 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 aplicativos (programas) dos seus ativos.

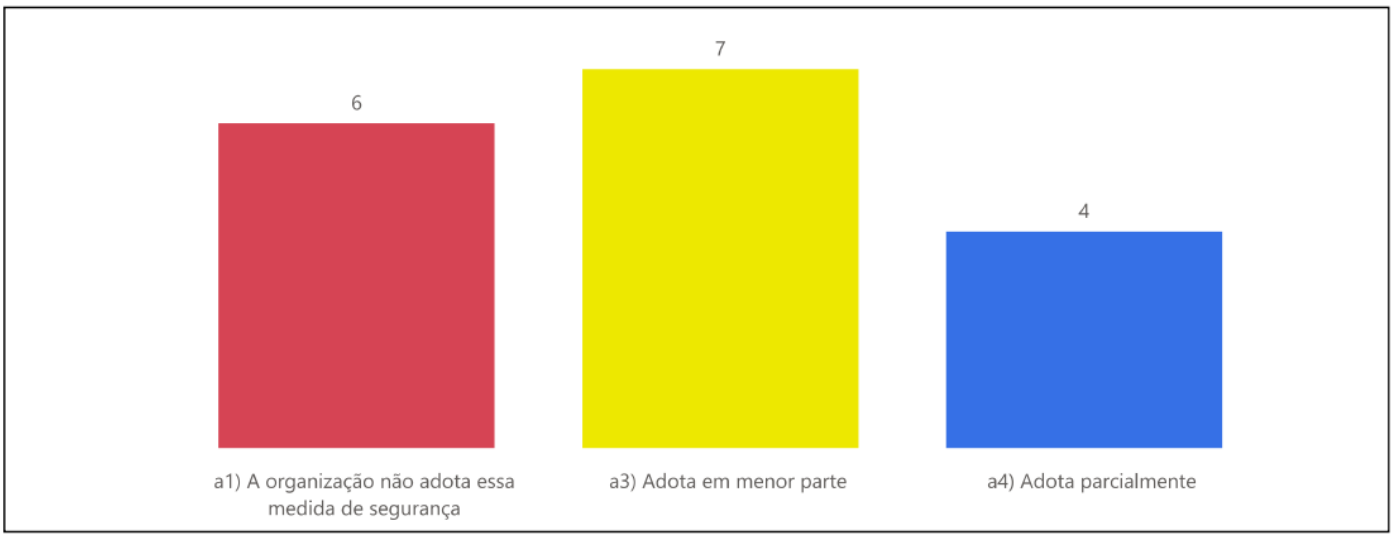

Figura 14 - Distribuição das respostas à **Questão 7.4.1** -
A organização executa a gestão automatizada da aplicação de correções (*patches*) nos aplicativos (programas) dos seus ativos?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Controle 14 - Conscientização sobre segurança e treinamento de competências

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.

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.

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.

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.

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

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

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Figura 15 - iControle14 e medidas de segurança correspondentes
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: : estabelecer e manter um 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.

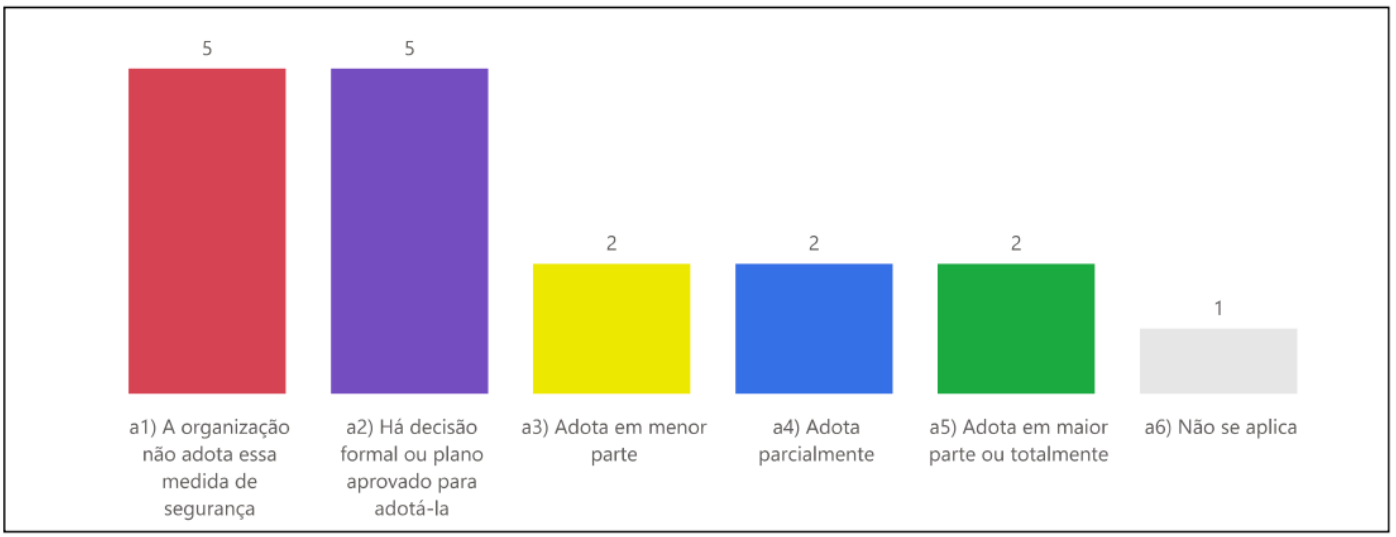

Figura 16 - Distribuição das respostas à **Questão 14.1.1** -
A organização estabelece e mantém um programa de conscientização em segurança?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

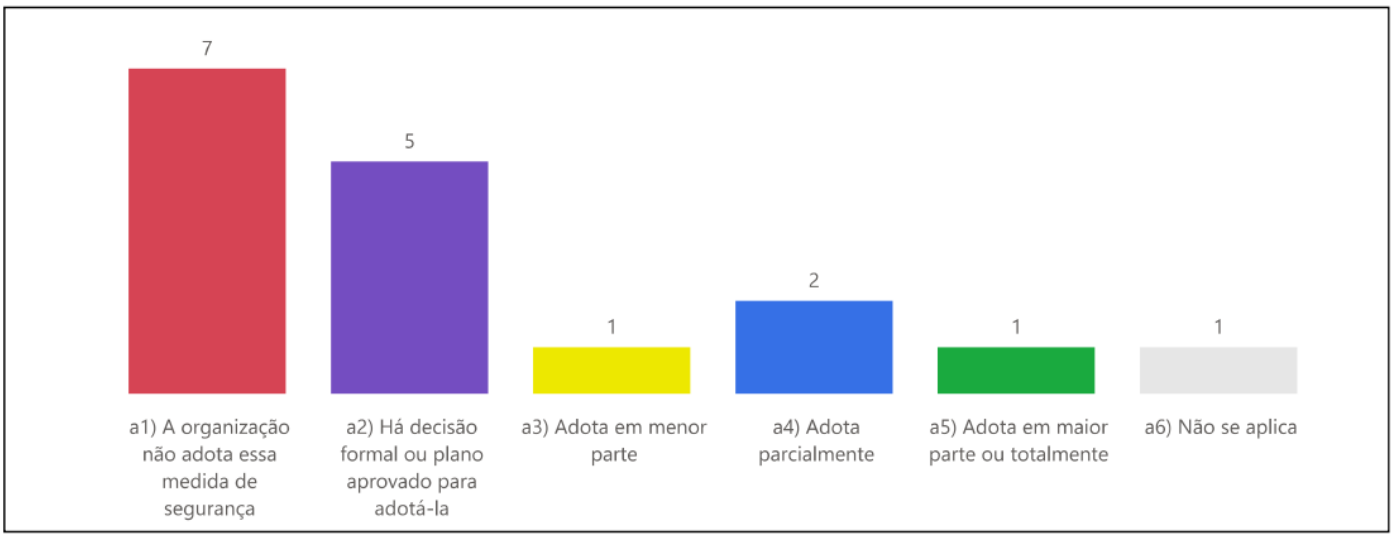

Figura 17 - Distribuição das respostas à **Questão 14.2.1** -
A organização treina seus colaboradores para reconhecerem ataques de engenharia social?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

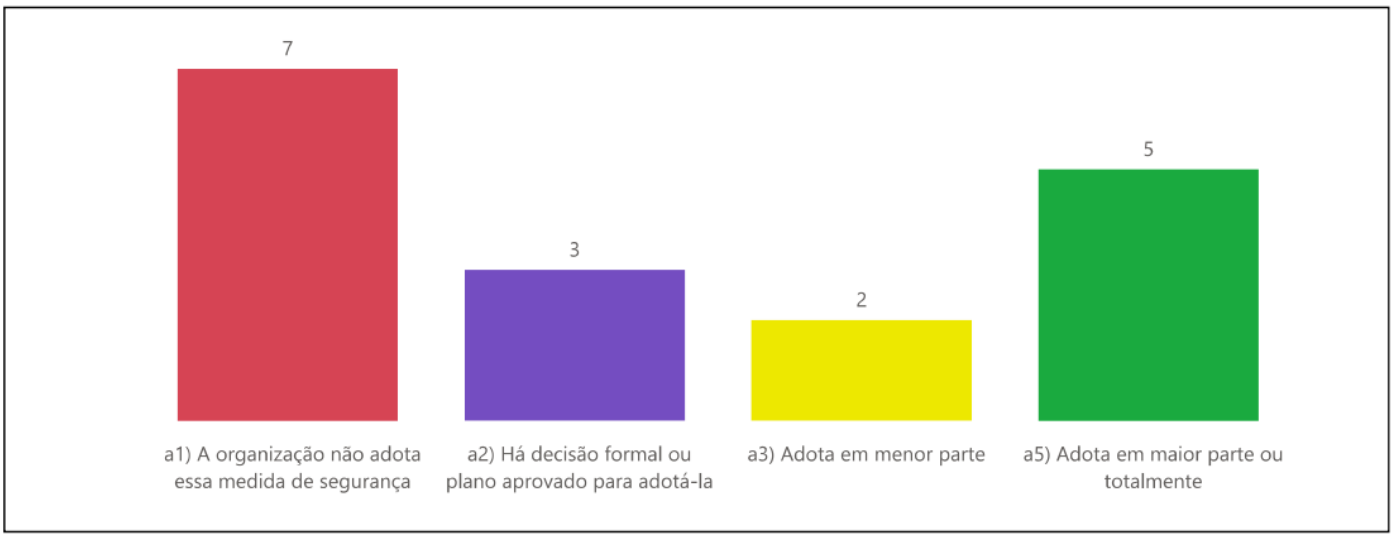

Figura 18 - Distribuição das respostas à **Questão 14.3.1** -
A organização treina seus colaboradores em melhores práticas de autenticação de usuários?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

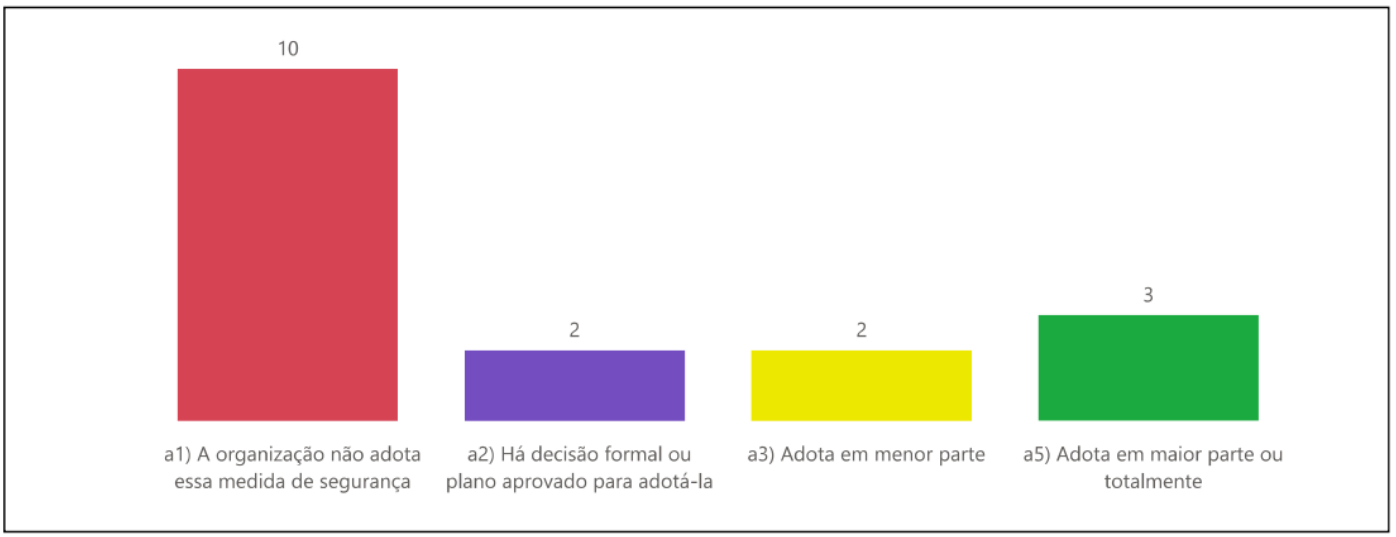

Figura 19 - Distribuição das respostas à **Questão 14.4.1** -
A organização treina seus colaboradores em melhores práticas de tratamento de dados?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

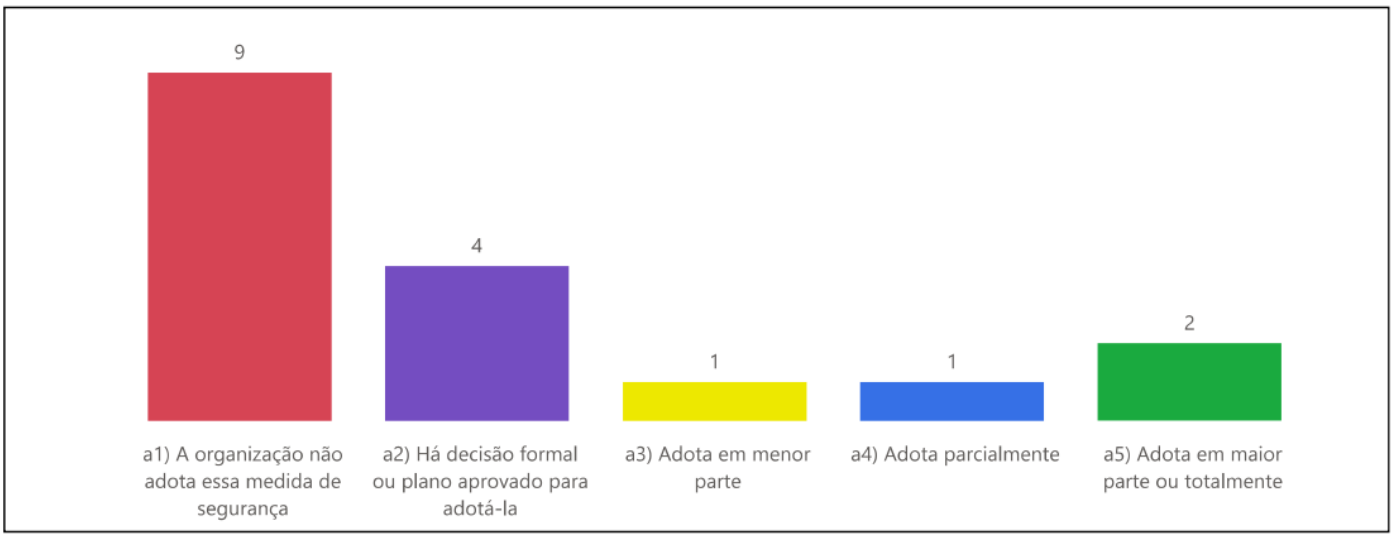

Figura 20 - Distribuição das respostas à **Questão 14.5.1** -
A organização treina seus colaboradores para evitarem exposição não intencional de dados?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

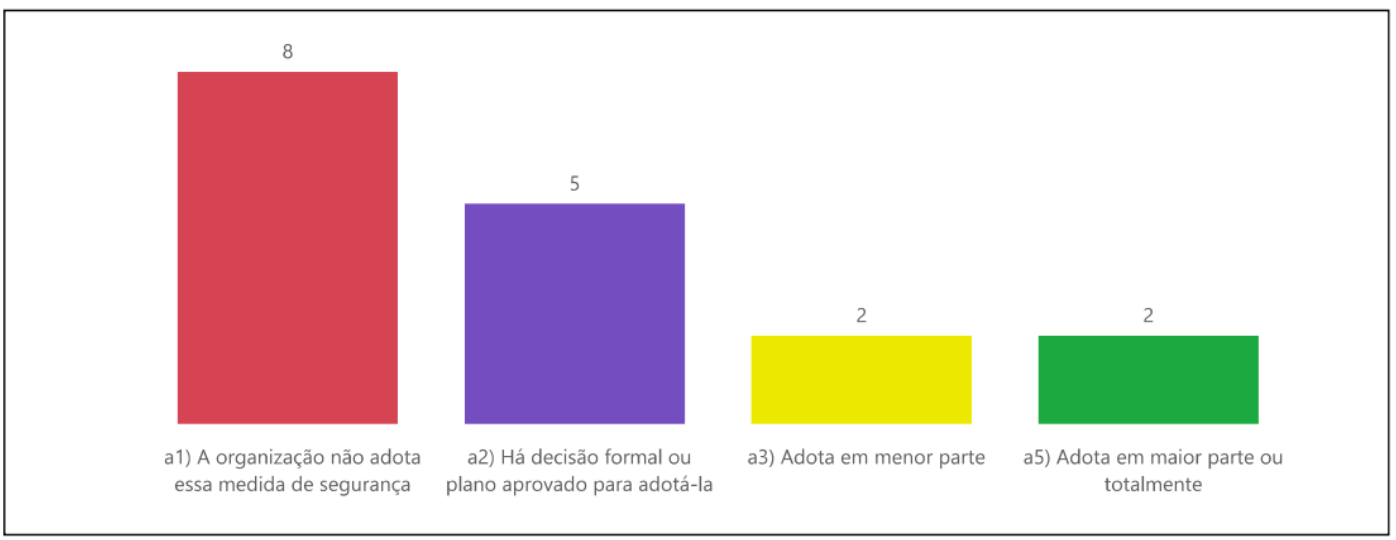

Figura 21 - Distribuição das respostas à **Questão 14.6.1** -
A organização treina seus colaboradores para reconhecerem e notificarem incidentes de segurança?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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).

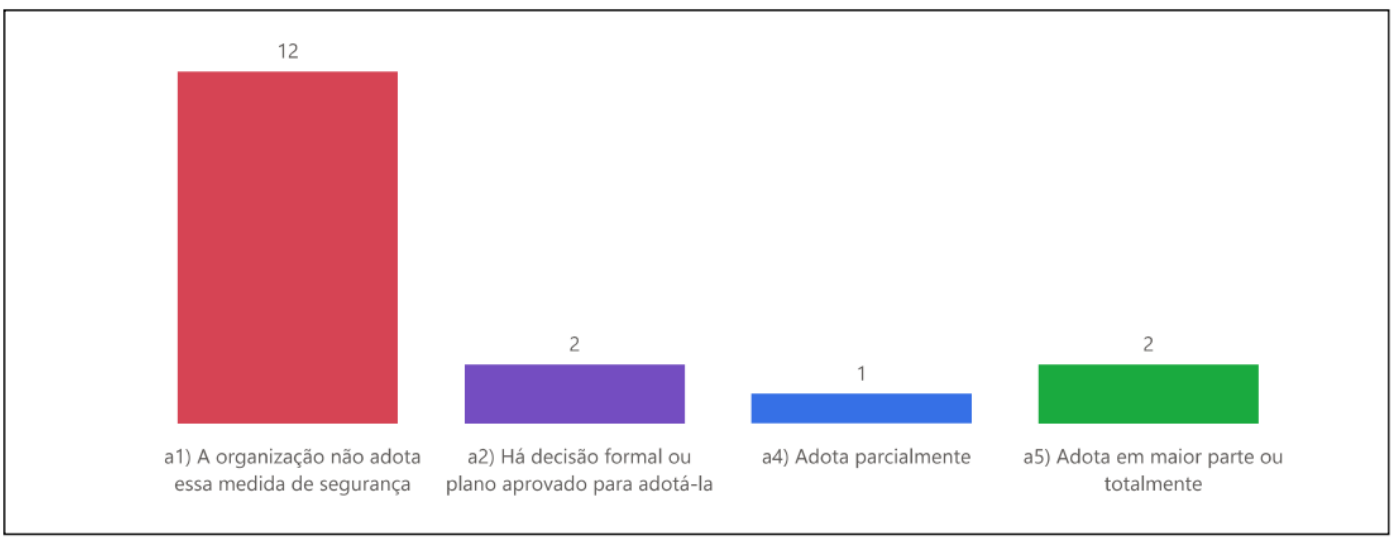

Figura 22 - Distribuição das respostas à **Questão 14.7.1** -
A organização treina seus colaboradores para identificarem e notificarem a falta de atualizações de segurança nos ativos corporativos?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: treinar os 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*).

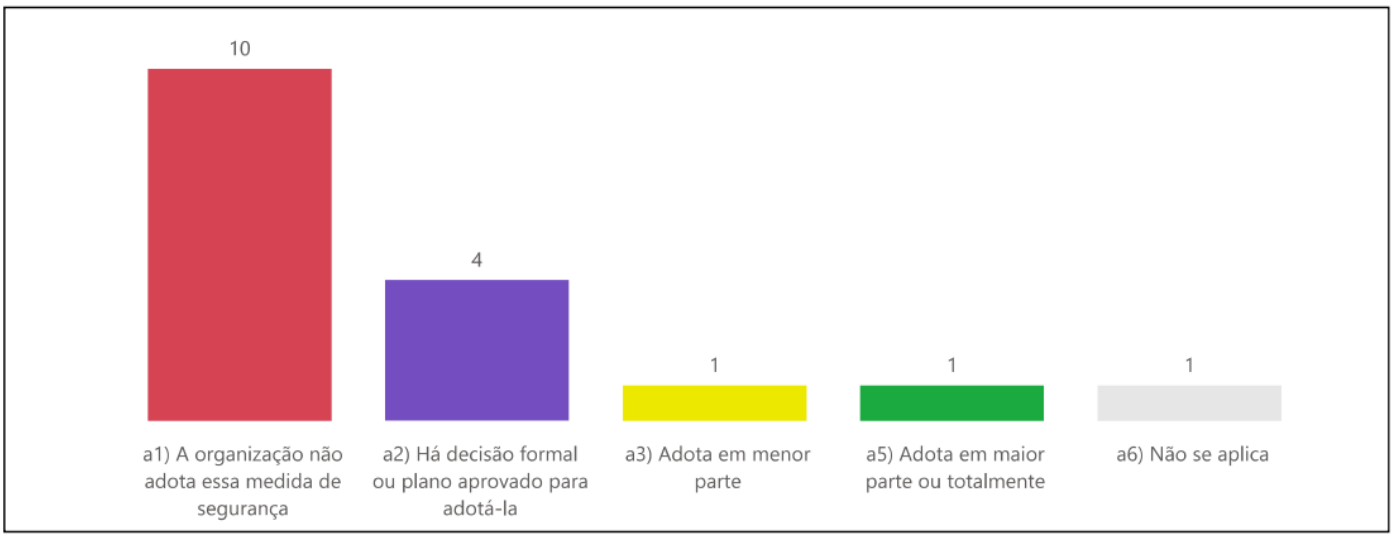

Figura 23 - Distribuição das respostas à **Questão 14.8.1** -
A organização treina seus colaboradores sobre os perigos de se conectar e transmitir dados corporativos por meio de redes inseguras?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

Controle 17 - Gestão de respostas a incidentes

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.

Tendo em vista que não se pode esperar que nenhuma organização esteja 100% protegida o tempo todo, cedo ou tarde incidentes ocorrerão. Assim, elaborar e manter um plano de resposta é essencial para que a organização esteja preparada quando isso acontecer. 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 prejuízos e recuperar dados e sistemas eventualmente corrompidos.

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

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.

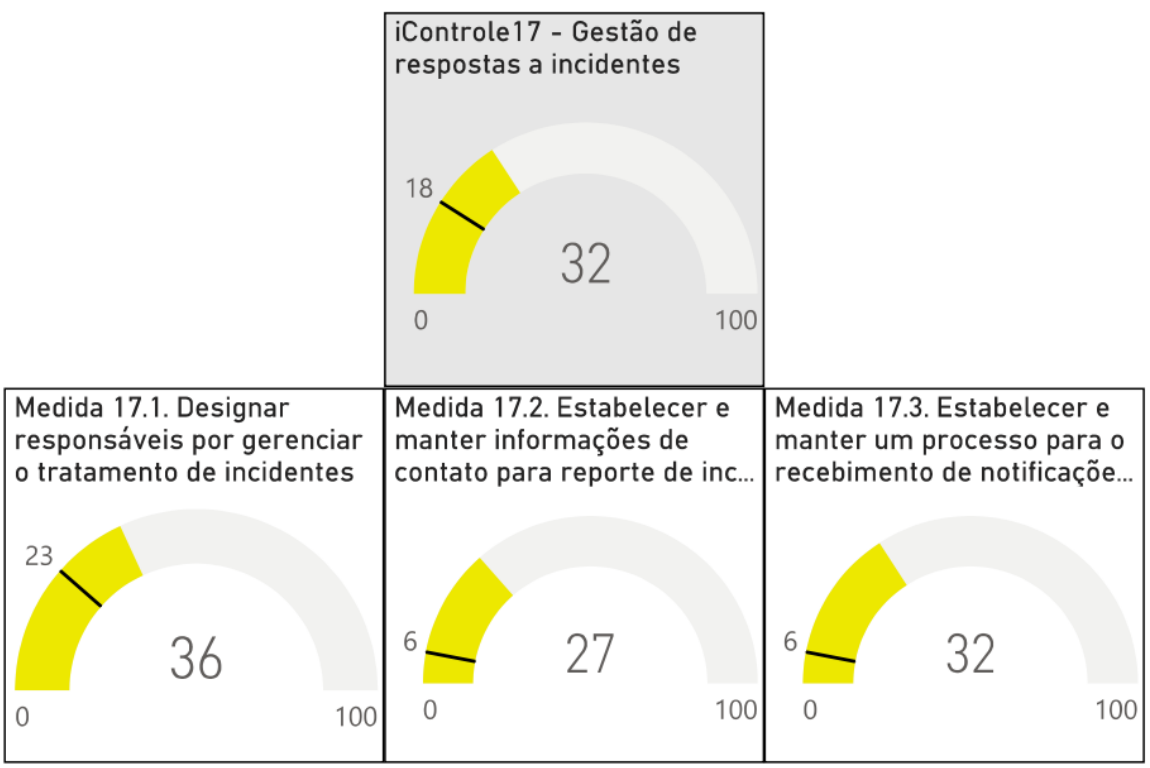

Figura 24 - iControle17 e medidas de segurança correspondentes
(valores médios e medianos)

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: designar responsáveis por gerenciar o processo de tratamento de incidentes.

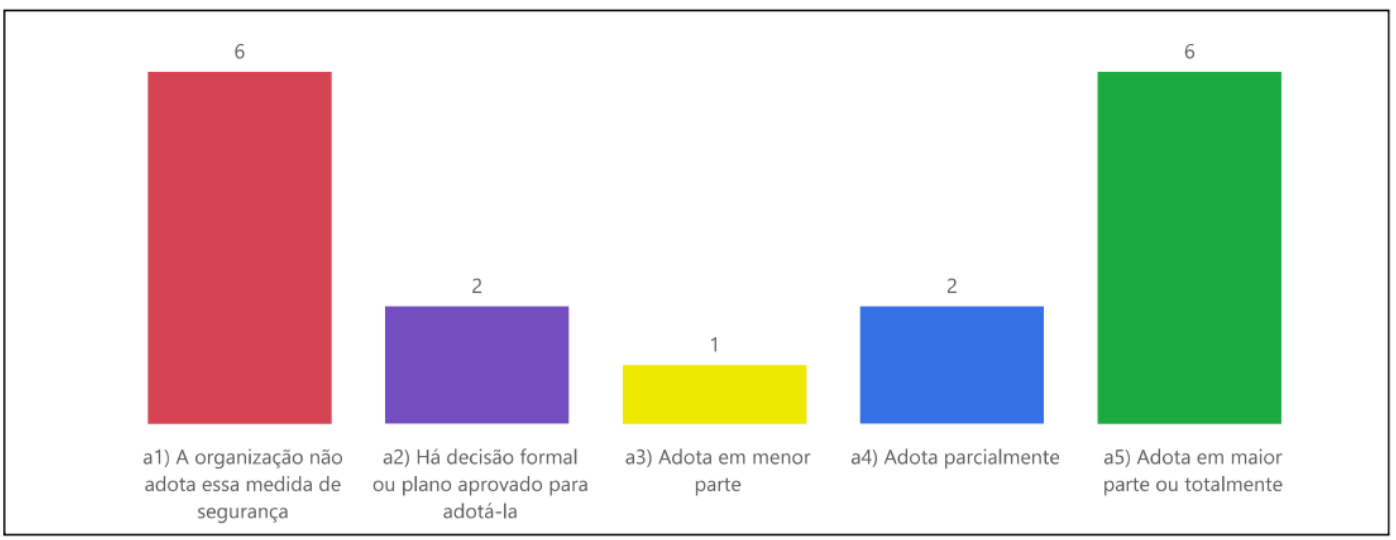

Figura 25 - Distribuição das respostas à **Questão 17.1.1** -
A organização designa responsáveis por gerenciar o processo de tratamento de incidentes?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter 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).

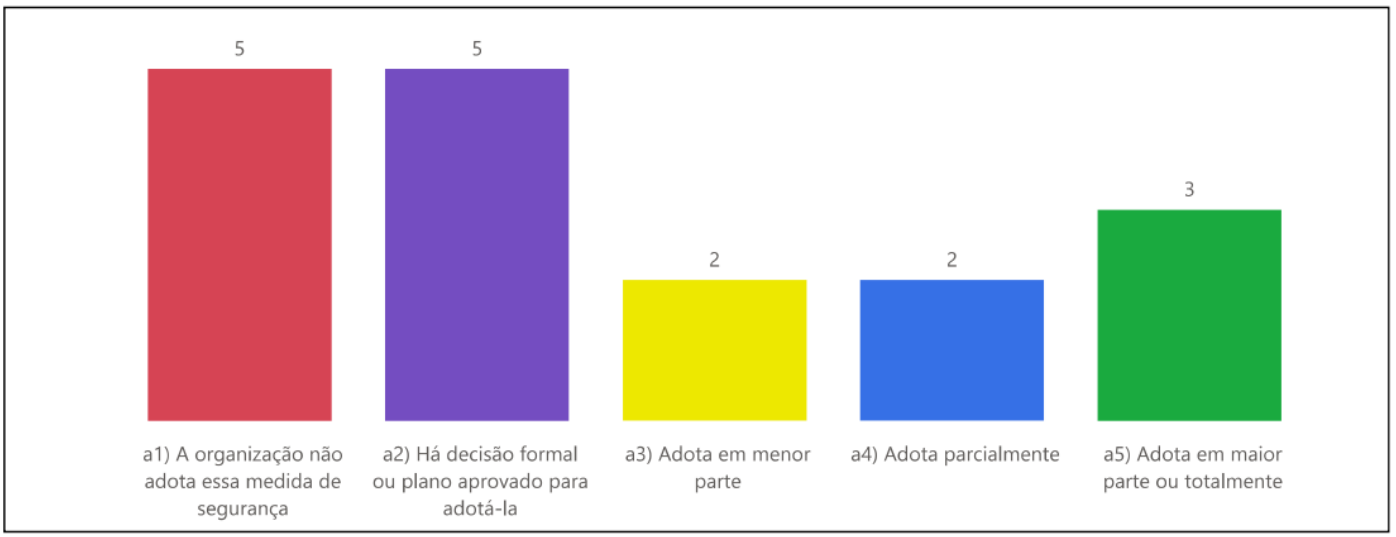

Figura 26 - Distribuição das respostas à **Questão 17.2.1** -
A organização estabelece e mantém informações de contato para reporte de incidentes de segurança?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.

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

Visão geral: estabelecer e manter 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).

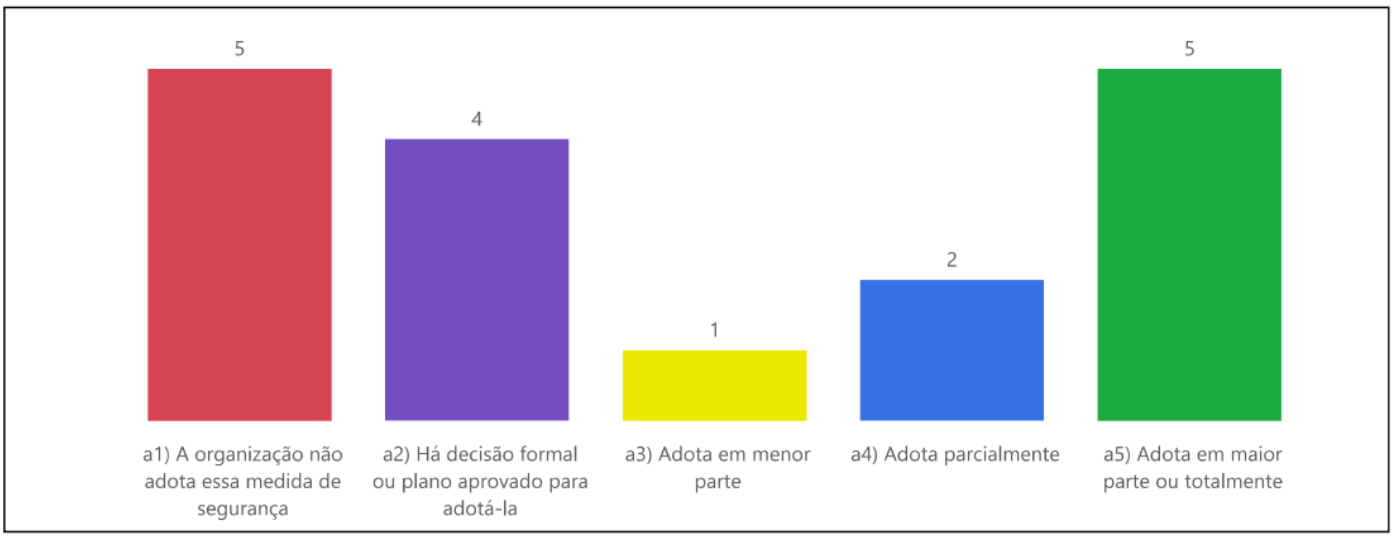

Figura 27 - Distribuição das respostas à **Questão 17.3.1** -
A organização estabelece e mantém um processo para que os colaboradores possam notificar incidentes de segurança?

Para verificar as assinaturas, acesse www.tcu.gov.br/autenticidade, informando o código 73106764.