TRIBUNAL DE CONTAS DA UNIÃO

10100
010011
10100

Cinco controles de segurança cibernética para ontem

10100
010011
10100

10100
010011
10100

REPÚBLICA FEDERATIVA DO BRASIL
TRIBUNAL DE CONTAS DA UNIÃO

MINISTROS

Ministro Bruno Dantas, Presidente em exercício
Ministro Walton Alencar Rodrigues
Ministro Benjamin Zymler
Ministro Augusto Nardes
Ministro Aroldo Cedraz
Ministro Vital do Rêgo
Ministro Jorge Oliveira
Ministro Antônio Anastasia

MINISTROS-SUBSTITUTOS

Ministro Augusto Sherman
Ministro Marcos Bemquerer
Ministro Weder de Oliveira

MINISTÉRIO PÚBLICO JUNTO AO TCU

Cristina Machado da Costa e Silva, Procuradora-Geral
Lucas Rocha Furtado, Subprocurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Marinus Eduardo de Vries Marsico, Procurador
Júlio Marcelo de Oliveira, Procurador
Sergio Ricardo Costa Caribé, Procurador
Rodrigo Medeiros de Lima, Procurador

TRIBUNAL DE CONTAS DA UNIÃO

Cinco controles de segurança cibernética para ontem

Brasília, 2022

http://www.tcu.gov.br
SAFS, Quadra 4, Lote 01
CEP 70042-900 – Brasília/DF

Brasil. Tribunal de Contas da União.
Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília : TCU, 2022.
36 p. : il. color.

1. Cibernética. 2. Segurança da informação. 3. Governo eletrônico. 4. Cibercrime. 5. Vulnerabilidade (segurança da informação). I. Título.

Ficha catalográfica elaborada pela Biblioteca Ministro Ruben Rosa

SUMÁRIO


10100
010011
10100
10100
010011
10100
10100
010011
10100
10100
010011
10100
10100
010011
10100

CINCO CONTROLES DE SEGURANÇA CIBERNÉTICA PARA ONTEM

O processo de transformação digital do governo, ao mesmo tempo em que disponibiliza progressivamente aos cidadãos informações e serviços digitalizados, acessíveis por meio de aplicativos e/ou sítios na internet, torna as organizações públicas ainda mais dependentes de soluções de tecnologia da informação (TI) – *softwares*, bases de dados e sistemas informatizados –, providas por sistemas relevantes e críticos, essenciais para o funcionamento do governo. Nesse cenário, vulnerabilidades e falhas de Segurança da Informação (SegInfo) e Segurança Cibernética (SegCiber) aumentam muito os riscos de ameaças e ataques cibernéticos, o que afeta significativamente o governo e os cidadãos.

Além disso, a pandemia causada pela covid-19 forçou as organizações a expandir rapidamente o regime de trabalho remoto, o que aumentou a quantidade de acessos externos às redes e o número de incidentes relacionados a ataques cibernéticos, em especial por meio de códigos maliciosos (*malware*[1]). Para se ter uma ideia, o Brasil foi o quinto país do mundo com maior incidência de ataques de *ransomware*[2] ("sequestro" de dados). Os ataques dispararam em 2020 e aumentaram 90% em 2021[3][4][5].

---

1 Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br). **Cartilha de segurança para internet** – fascículo códigos maliciosos. Março de 2017, 8p. Disponível em: <https://cartilha.cert.br/fasciculos/codigos-maliciosos/fasciculo-codigos-maliciosos.pdf>. Acesso em: 2 fev. 2022.

2 Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cert.br). **Cartilha de segurança para internet – *ransomwareransomware***. Disponível em: <https://cartilha.cert.br/ransomware>. Acesso em: 2 fev. 2022.

3 EUA. SonicWall Inc. Mid-Year Update: 2021 SonicWall Cyber Threat Report, p. 9. Milpitas - CA - EUA: SonicWall Inc., 2021, 29p. Disponível em: <https://www.sonicwall.com/2021-cyber-threat-report>. Acesso em: 2 fev.2022.

4 Disponível em: <https://olhardigital.com.br/coronavirus/noticia/ataques-de-ransomware-no-brasil-cresceram-3-5x-desde-janeiro-diz-kaspersky/98583>. Acesso em: 2 fev. 2022.

5 Disponível em: <https://tiinside.com.br/21/05/2021/ataques-de-ransomware-aumentaram-90-entre-2020-e-2021-alerta-sonicwall-capture-labs>. Acesso em: 2 fev. 2022.

Recentes incidentes cibernéticos ocorridos em algumas organizações públicas federais, especialmente no Ministério da Saúde (MS), em dezembro de 2021, ilustram a importância da gestão de SegCiber e os impactos decorrentes de falhas e vulnerabilidades em sítios e sistemas críticos de governo, tanto em cada organização pública individualmente quanto, de modo sistêmico e colaborativo, em toda a Administração Pública.

Esse cenário de exposição das organizações a riscos crescentes, quer por falhas na gestão da SegInfo, quer por implementação insuficiente de controles de SegCiber, já havia sido registrado no Acórdão 4.035/2020-TCU-Plenário (levantamento da governança e gestão de SegInfo e SegCiber da Administração Pública federal), de relatoria do ministro Vital do Rêgo[6], cujo relatório sugeriu a Estratégia de fiscalização do TCU em SegInfo e SegCiber 2020-2023[7] e previu fiscalização – autorizada no Acórdão 1.109/2021-TCU-Plenário (*auditoria de backup/restore* dos órgãos e das entidades da Administração Pública federal), de relatoria do ministro Vital do Rêgo – para acompanhar a adoção, pelas organizações públicas federais, de controles críticos de SegCiber.

Por meio deste acompanhamento (Acórdão 1768/2022-TCU-Plenário, de relatoria do ministro Vital do Rêgo), o TCU visa a contribuir para a transformação digital do país, conscientizando os gestores públicos de SegInfo acerca dos riscos aos quais as organizações estão sujeitas, em virtude dos ataques e incidentes cibernéticos, cada vez mais frequentes, de modo que sejam implementados controles e medidas de segurança adequados para endereçá-los.

A referência de boas práticas de SegCiber utilizada no acompanhamento é a versão 8 do *framework* do *Center for Internet Security* (CIS)[8], organização independente e sem fins lucrativos que recomenda um total de 18 controles crí-

---

6 BRASIL. Tribunal de Contas da União (TCU). **Acórdão 4.035/2020-TCU-Plenário.** Relator: Ministro Vital do Rêgo. Brasília: TCU, 8/12/2020. Disponível em: <https://pesquisa.apps.tcu.gov.br/#/documento/acordao- completo/*/NUMACORDAO%253A4035%2520ANOACORDAO%253A2020/DTRELEVANCIA%2520desc%252C%2520NUMACORDAOINT%2520desc/0>. Acesso em: 2 fev. 2022.

7 BRASIL. Tribunal de Contas da União (TCU). **Estratégia de fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023.** Brasília: TCU, 2021. Disponível em: <https://portal.tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm>. Acesso em: 2 fev. 2022.

8 Disponível em: <https://www.cisecurity.org/controls/v8>. Acesso em: 2 fev. 2022.

ticos de SegCiber (Quadro 1), os quais formam um conjunto de ações de defesa de alta prioridade contra ataques cibernéticos mais pervasivos. São ações consideradas imprescindíveis e urgentes para toda organização que busca melhorar a própria SegCiber.

Assim, os controles e as medidas de segurança preconizados pelo CIS serão progressivamente avaliados pelo TCU ao longo de sete ciclos. No primeiro ciclo de acompanhamento, foram avaliados os cinco controles negritados no Quadro 1.

Quadro 1: **Controles críticos de SegCiber preconizados pelo CIS**

1	**Inventário e controle de ativos corporativos**
2	**Inventário e controle de ativos de *software***
3	Proteção de dados
4	Configuração segura de ativos corporativos e *software*
5	Gestão de contas
6	Gestão de controles de acesso
7	**Gestão contínua de vulnerabilidades**
8	Gestão de registros (*logs*) de auditoria
9	Proteção de *e-mail* e navegador da web
10	Defesa contra *malware*
11	Recuperação de dados
12	Gestão de infraestrutura de rede
13	Monitoramento e defesa de rede
14	**Conscientização sobre segurança e treinamento de competências**
15	Gestão de provedores de serviço
16	Segurança de aplicações de *software*
17	**Gestão de respostas a incidentes**
18	Teste de invasão

Fonte: CIS Controls® Version 8 (tradução livre).

Qual a finalidade de cada um desses cinco controles?

- **Controle 1 – Inventário e controle de ativos corporativos:** identificar e impedir a utilização de ativos de TI não autorizados/gerenciados como vetores de ataques cibernéticos.
- **Controle 2 – Inventário e controle de ativos de *software*:** identificar e impedir a utilização de *softwares* não autorizados/gerenciados como vetores de ataques cibernéticos.
- **Controle 7 – Gestão contínua de vulnerabilidades:** evitar a exploração de vulnerabilidades conhecidas nos ativos corporativos de TI.
- **Controle 14 – Conscientização sobre segurança e treinamento de competências:** reduzir a possibilidade de incidentes e ataques derivados do comportamento humano – engenharia social.
- **Controle 17 – Gestão de respostas a incidentes:** melhorar a capacidade de identificar potenciais ameaças e ataques, evitar que se espalhem e recuperar rapidamente dados e sistemas eventualmente corrompidos.

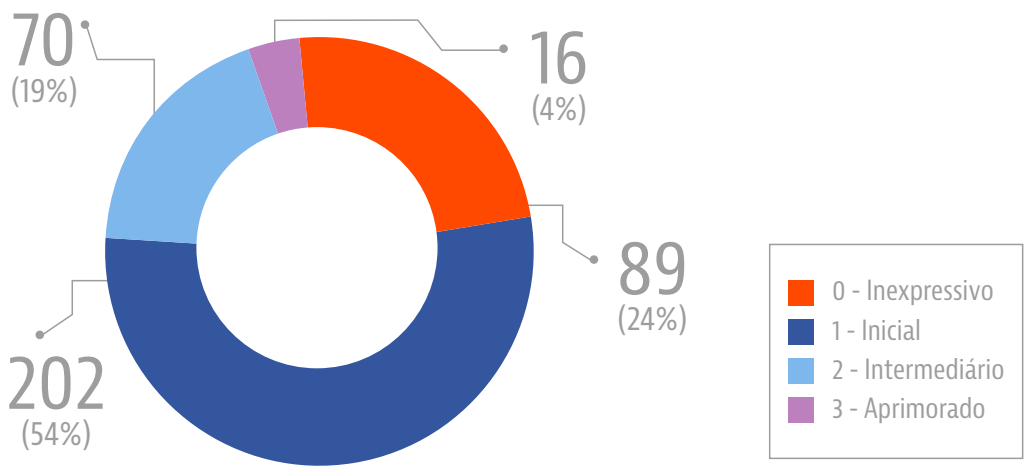
O método utilizado na fiscalização foi a autoavaliação de controles internos – *Control Self-Assessment* (CSA). Os gestores receberam um questionário para preencher com respostas que melhor refletissem a situação atual das respectivas organizações em relação aos cinco controles. Esse primeiro ciclo de acompanhamento recebeu respostas de 377 organizações públicas federais.

De modo a representar as respostas das organizações em valores numéricos que variassem de 0 a 100, foram calculados os indicadores **iControle1, iControle2, iControle7, iControle14, iControle17** e **iSegCiber**, para sintetizar a maturidade geral das organizações nos cinco controles de SegCiber[9].

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 SegCiber: **Inexpressivo** (iSegCiber ≤ 15), **Inicial** (15 < iSegCiber ≤ 50), **Intermediário** (50 < iSegCiber ≤ 80) e **Aprimorado** (iSegCiber > 80), resultando no indicador **nSegCiber**.

O panorama geral que se apresentou neste primeiro ciclo é preocupante, pois 24% das 377 organizações ainda se encontram no estágio **Inexpressivo** e 54%, no estágio **Inicial**, conforme apresentado no Gráfico 1.

Gráfico 1: **Distribuição das organizações em função do nSegCiber**



Fonte: Elaboração própria.

9 O método de cálculo dos indicadores é explicado no relatório de fiscalização, capítulo 7, tópico Indicadores de SegCiber.

De modo semelhante, as respostas das organizações avaliadas indicam que ainda é **Inicial** o nível médio de maturidade em SegCiber, calculado em função de todos os indicadores numéricos (Figura 1).

Figura 1: Valores médios e medianos dos indicadores: iSegCiber, iControle1, iControle2, iControle7, iControle14 e iControle17

Fonte: Elaboração própria.

Os resultados indicam uma situação de alto risco para a SegCiber do setor público federal, o que justifica a implementação urgente dos 18 controles críticos do CIS e, em especial **para ontem**, dos cinco controles avaliados neste primeiro ciclo de acompanhamento, visando à proteção contra ameaças cibernéticas e redução da probabilidade de invasões.

Cada um desses controles é descrito a seguir, incluindo as respectivas medidas de segurança básicas preconizadas pelo CIS e algumas sugestões de boas práticas adicionais que podem ser adotadas.

As medidas de segurança são ações específicas que as empresas devem realizar para implementar um controle. O CIS prioriza as medidas de segurança em três grupos de implementação: básicas (iG1), intermediárias (iG2) e avançadas (iG3). Neste primeiro ciclo de acompanhamento, só foram avaliadas as medidas básicas, que são aquelas que **todas as empresas** devem implementar para se proteger dos ataques mais comuns. As sugestões de boas práticas adicionais foram identificadas no próprio *framework* do CIS e em outras referências, como a norma ABNT NBR ISO/IEC 27002:2013.

Além disso, o Apêndice I traz indicações de outras normas de referência em SegInfo que também podem auxiliar os gestores e o Apêndice II, um quadro com subpráticas que devem ser implementadas ao se adotar cada medida de segurança.

CONTROLE 1 – INVENTÁRIO E CONTROLE DE ATIVOS CORPORATIVOS

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

Por que esse controle é crítico?

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

Medidas de segurança básicas

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

Estabelecer e manter inventário 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.

Medida de segurança 1.2 - Tratar ativos não autorizados

Ao identificar ativo não autorizado, escolher entre remover o ativo da rede, impedir que o ativo se conecte novamente à rede ou colocar o ativo em quarentena.

Boas práticas adicionais

Para identificar equipamentos não autorizados, devem-se utilizar ferramentas de descoberta ativa e passiva e *logs* (registros) do *Dynamic Host Configuration Protocol* (DHCP), para atualização do inventário de ativos corporativos, semanalmente ou com mais frequência. Ferramentas de descoberta ativa são aquelas que coletam dados interagindo diretamente com os equipamentos monitorados. Ferramentas de descoberta passiva são aquelas que coletam dados de *logs* e notificações *trap* – *Simple Network Management Protocol* (SNMP) ou mensagens retransmitidas pelo equipamento monitorado para um agente passivo.

CONTROLE 2 – INVENTÁRIO E CONTROLE DE ATIVOS DE *SOFTWARE*

Gerenciar ativamente (registrar, acompanhar e corrigir) todo *software* – sistemas operacionais e aplicativos – utilizado, de modo que *softwares* autorizados possam ser instalados e executados nas máquinas e *softwares* não autorizados/gerenciados possam ser detectados e tenham a instalação/execução impedida.

Por que esse controle é crítico?

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

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

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

Medidas de segurança básicas

Medida de segurança 2.1 – Estabelecer e manter inventário de *software*

Estabelecer e manter inventário detalhado de *software*, com informações precisas, detalhadas e atualizadas sobre todos os *softwares* instalados nos ativos da organização necessários para realização das tarefas e rotinas corporativas diárias.

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

Assegurar que apenas *software* atualmente suportado – previamente testado e homologado pelo setor de TI – seja designado como autorizado no inventário de *software*.

Medida de segurança 2.3 – Tratar *softwares* não autorizados

Tratar *software* não autorizado, ou seja, *software* não suportado para o qual não tenha sido documentada exceção.

Boas práticas adicionais

A documentação de exceções para permitir o uso de *software* não autorizado deve ser utilizada com bastante cautela. A partir da documentação de determinado número de exceções relacionadas ao mesmo *software* ou, a depender do caso, de uma única exceção, convém que o setor de TI avalie a possibilidade de testá-lo e homologá-lo, de modo que 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 utilizar ferramentas que automatizam o processo de descoberta e documentação (inventário) dos *softwares* presentes e implementar controles técnicos (lista de permissão, assinatura digital, 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

Desenvolver 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 oportunidades para eventuais atacantes. Importante, também, monitorar constantemente fontes públicas e privadas de informações sobre novas ameaças e vulnerabilidades.

Por que esse controle é crítico?

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 respectivas medidas de mitigação, de modo que possam, regularmente, avaliar os ambientes de 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 seus *softwares* à procura de vulnerabilidades e corrige proativamente as falhas encontradas corre sério risco de, cedo ou tarde, ter seus ativos comprometidos.

Medidas de segurança básicas

Medida de segurança 7.1 – Estabelecer e manter processo de gestão de vulnerabilidades

Estabelecer e manter processo contínuo de avaliação e monitoramento dos ativos de *hardware* e *software*, com vistas a eliminar, mitigar ou corrigir vulnerabilidades e aprimorar configurações, controles e táticas de defesa.

Medida de segurança 7.2 – Estabelecer e manter processo de correção de vulnerabilidades

Estabelecer e manter 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.

Medida de segurança 7.3 – Executar gestão automatizada de correção (*patches*) de sistemas operacionais

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.

Medida de segurança 7.4 – Executar gestão automatizada de correção (*patches*) de aplicativos

Executar gestão automatizada da aplicação de correções/*patches* nos aplicativos (programas) de seus ativos.

Boas práticas adicionais

Os processos de gestão e correção de vulnerabilidades podem ser vistos como subfunções do processo de gestão de mudanças da organização e, portanto, aproveitar-se das práticas e dos procedimentos a ele 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 *Information Technology Infrastructure Library* (ITIL) v. 3, *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 de varreduras completas de vulnerabilidades, incluindo ativos internos da organização e externos a ela, autenticadas e não autenticadas, e realizar as respectivas correções, sempre que possível. Preferencialmente, tais ferramentas devem adotar definições padronizadas, baseadas no *Security Content Automation Protocol* (SCAP).

Sobre a aplicação de correções (*patches*), como os fornecedores estão, cada vez mais, sendo pressionados a liberar esses pacotes com brevidade, é muito importante, antes da respectiva aplicação, atestar que o problema em questão será adequadamente resolvido e não serão causados efeitos colaterais indesejáveis. 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 impactando a continuidade do negócio. Se a organização não tiver condições de conduzir tais testes, de maneira satisfatória, por conta própria, deve atrasar a aplicação da correção, para avaliar os riscos associados, a partir das experiências relatadas por outros usuários/outras organizações.

CONTROLE 14 – CONSCIENTIZAÇÃO SOBRE SEGURANÇA E TREINAMENTO DE COMPETÊNCIAS

Estabelecer e manter 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 que reduzam os riscos para a organização.

Por que esse controle é crítico?

No tripé da SegInfo, formado por tecnologia, processos e pessoas, estas 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 induzindo o usuário a clicar em um link ou abrir um anexo de e-mail e, com isso, instalar um *software* malicioso no próprio computador, do que explorando 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 destinatário errado, a perda de equipamento/dispositivo portátil – notebook, pendrive –, a utilização de senha fraca ou reutilização da mesma senha usada para autenticação em 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 o componente comportamento humano, visto que, mesmo de forma não intencional, o usuário pode causar incidente de segurança.

Medidas de segurança básicas

Medida de segurança 14.1 – Estabelecer e manter programa de conscientização em segurança

Estabelecer e manter programa contínuo e permanente de treinamento, com vistas a mostrar aos colaboradores os riscos e as ameaças aos quais os ativos e dados da organização estão sujeitos e como agir para evitá-los/mitigá-los.

Medida de segurança 14.2 – Treinar os colaboradores para reconhecer ataques de engenharia social

Treinar os colaboradores para reconhecer ataques de engenharia social, ou seja, manipulação psicológica de indivíduos para que executem ações que não deveriam ou, então, divulguem informações confidenciais, sigilosas ou sensíveis.

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

Treinar os colaboradores em melhores práticas de autenticação de usuários. A autenticação é o mecanismo pelo qual é possível confirmar a identidade do usuário.

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

Treinar os colaboradores em melhores práticas de tratamento de dados, o que envolve identificar dados sensíveis no contexto da organização e saber como armazená-los, transferi-los, arquivá-los e destruí-los adequadamente, de modo a minimizar os riscos de vazamento.

Medida de segurança 14.5 – Treinar os colaboradores para evitar exposição não intencional de dados

Treinar os colaboradores para evitar exposição não intencional de dados, como, por exemplo, a perda ou o extravio de dispositivos portáteis, o envio de informações sensíveis a destinatário errado e a publicação de dados para audiência que não deveria ter acesso a eles.

Medida de segurança 14.6 – Treinar os colaboradores para reconhecer e notificar incidentes de segurança

Treinar os colaboradores para reconhecer e notificar incidentes de segurança, ou seja, 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.

Medida de segurança 14.7 – Treinar os colaboradores para identificar e notificar falta de atualização de segurança nos ativos corporativos

Treinar os colaboradores para identificar e notificar falta de atualização de segurança nos ativos corporativos, como, por exemplo, ativos com versões de *software* desatualizadas e/ou sem a instalação dos pacotes de correções mais recentes e ativos em que a execução dos processos e das ferramentas automatizados de aplicação dessas correções tenha apresentado alguma falha ou erro.

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

Treinar os colaboradores sobre os perigos de se conectar a redes inseguras e transmitir dados corporativos por meio delas. São inseguras as redes que não implementam medidas básicas de segurança, como a autenticação de usuários e utilização de criptografia, e não são protegidas por soluções antivírus ou *firewalls*.

Boas práticas adicionais

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 impactos potenciais, positivos e negativos, dos diferentes comportamentos e** das condutas sobre a organização.

Ademais, é sempre importante testar os conhecimentos adquiridos pelos colaboradores ao final da realização de qualquer ação de conscientização, educação e/ou treinamento em segurança (da informação e cibernética), que pode fazer parte de atividade educacional de TI mais abrangentes ou, ainda, treinamento e curso de caráter mais geral em segurança.

CONTROLE 17 – GESTÃO DE RESPOSTAS A INCIDENTES

Estabelecer programa para desenvolver e manter capacidade de resposta a incidente de SegInfo, de modo a estar preparado para detectar ataques e responder rapidamente a eles. O programa compreende políticas, planos, procedimentos, definição de papeis, treinamento e comunicação.

Por que esse controle é crítico?

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

Medidas de segurança básicas

Medida de segurança 17.1 – **Designar responsáveis por gerenciar o tratamento de incidentes**

Designar responsáveis por gerenciar o processo de tratamento de incidentes.

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

Estabelecer e manter informações de contato para reporte de incidentes de segurança, tais como relação com as informações de contato de todos os *stakeholders* que precisam ser informados sobre a ocorrência dos incidentes.

Medida de segurança 17.3 – **Estabelecer e manter processo para recebimento de notificação de incidentes**

Estabelecer e manter processo para recebimento de notificação de incidentes de segurança, definindo requisitos mínimos, a exemplo dos atores, dos procedimentos, dos prazos e do conteúdo das notificações de incidentes.

Boas práticas adicionais

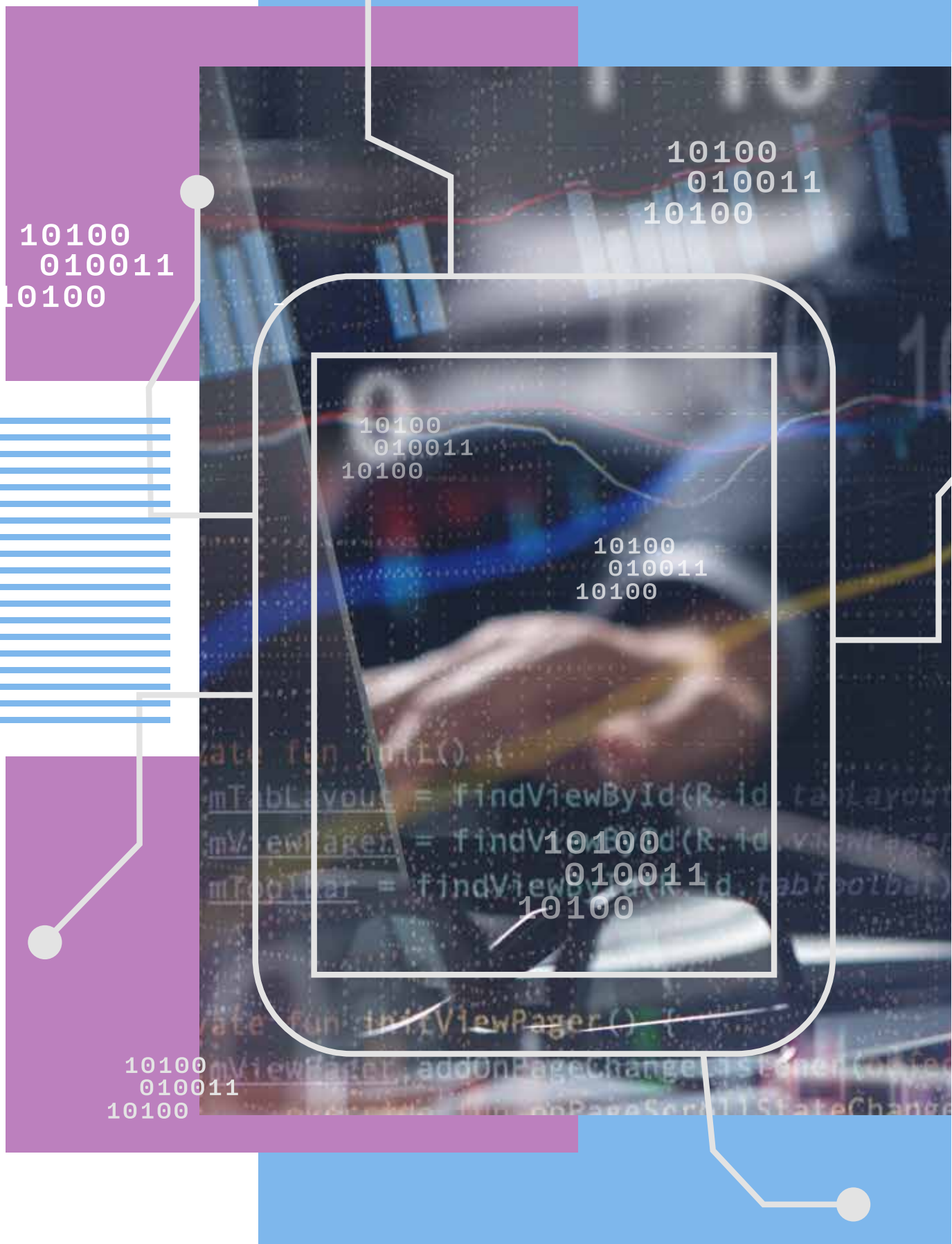
A equipe de resposta a incidentes deve realizar treinamento periódico baseado em cenários de ataque, ajustados para as ameaças e os impactos potenciais enfrentados pela organização, que ajudam a garantir que tanto a liderança corporativa quanto os membros da equipe técnica estejam sempre preparados para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

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

CONCLUSÃO

Este documento apresentou **cinco controles críticos** que a Administração Pública federal precisa implementar com urgência, **para ontem**, tendo em vista que a situação detectada no primeiro ciclo de acompanhamento do TCU sobre a SegCiber das organizações públicas federais é de alto risco.

O objetivo é conscientizar os gestores públicos e induzir a implementação de controles e medidas de segurança necessários para mitigar os riscos de ataques e incidentes decorrentes de vulnerabilidades e falhas de SegInfo e SegCiber, que, atualmente, podem prejudicar significativamente o governo e os cidadãos e impactar negativamente no processo de transformação digital do país.


10100
010011
10100
10100
010011
10100
10100
010011
10100
10100
010011
10100
10100
010011
10100
10100
010011
10100

APÊNDICE I
OUTRAS REFERÊNCIAS

CONTROLE 1 – INVENTÁRIO E CONTROLE DE ATIVOS CORPORATIVOS

O item 8 (gestão de ativos) da norma técnica ABNT NBR ISO/IEC 27002/2013 recomenda que os ativos associados à informação e aos recursos de processamento da informação sejam identificados e um inventário seja estruturado e mantido. Também recomenda que as responsabilidades pela proteção desses ativos sejam definidas.

A Instrução Normativa (IN) GSI/PR 3/2021 inclui o mapeamento de ativos de informação dentre os processos relacionados à gestão de SegInfo que devem ser observados pelos órgãos e pelas entidades da Administração Pública federal (art. 3º), com objetivo de estruturar e manter registro de ativos de informação, destinado a subsidiar os processos de gestão de riscos, continuidade e mudança nos aspectos relativos à SegInfo (art. 4º). Nos termos do art. 9º da referida IN, a gestão dos ativos de informação deve: identificar e classificar os ativos por níveis de criticidade; identificar potenciais ameaças aos ativos; identificar vulnerabilidades dos ativos; e avaliar os riscos dos ativos ou grupos de ativos.

CONTROLE 2 – INVENTÁRIO E CONTROLE DE ATIVOS DE *SOFTWARE*

Além das referências citadas no controle anterior, relativas à identificação de ativos de modo geral, destaca-se que o item 12.6.2 (restrições quanto à instalação de *software*) da norma técnica ABNT NBR ISO/IEC 27002:2013 recomenda que "sejam estabelecidas e implementadas regras definindo critérios para instalação de *software* pelos usuários", tendo em vista que a instalação de *softwares* não autorizados pode trazer riscos, a partir da introdução de vulnerabilidades que, em última análise, podem resultar em incidentes de segurança como vazamento ou perda da integridade de dados e violação de propriedade intelectual.

CONTROLE 7 – GESTÃO CONTÍNUA DE VULNERABILIDADES

O item 12.6.1 (gestão de vulnerabilidades técnicas) da norma técnica ABNT NBR ISO/IEC 27002:2013 recomenda que "informações sobre vulnerabilidades técnicas dos sistemas de informação em uso na organização sejam obtidas em tempo hábil". Também recomenda que a exposição a essas vulnerabilidades "seja avaliada e sejam tomadas as medidas apropriadas para lidar com os riscos associados".

CONTROLE 14 – CONSCIENTIZAÇÃO SOBRE SEGURANÇA E TREINAMENTO DE COMPETÊNCIAS

O item 7.2.2 (conscientização, educação e treinamento em SegInfo) da norma técnica ABNT NBR ISO/IEC 27002:2013 recomenda que "os funcionários da organização e, onde pertinente, as partes externas recebam treinamento, educação e conscientização apropriados, bem como atualizações regulares de políticas e procedimentos organizacionais relevantes para as funções que exercem".

De acordo com o item 5.1 da Norma Complementar 18/IN01/DSIC/GSIPR (diretrizes para as atividades de ensino em SegInfo e comunicações nos órgãos e nas entidades da Administração Pública federal), "os agentes públicos devem receber orientações/instruções, no período de ambientação e formação inicial ou continuada, nos órgãos ou nas entidades em que atuam, por meio de atividades de ensino de sensibilização, conscientização, capacitação e especialização (...)".

CONTROLE 17 – GESTÃO DE RESPOSTAS A INCIDENTES

De acordo com o item 16 (gestão de incidentes de SegInfo) da norma técnica ABNT NBR ISO/IEC 27002:2013, a gestão de incidentes de SegInfo tem como objetivo "assegurar um enfoque consistente e efetivo para gerenciar os incidentes de SegInfo, incluindo a comunicação sobre fragilidades e eventos". O subitem 16.1.1 (responsabilidades e procedimentos) da mesma norma recomenda que "responsabilidades e procedimentos de gestão sejam estabelecidos, para assegurar respostas rápidas, efetivas e coordenadas aos incidentes de SegInfo".

Conforme o item 2.1 da Norma Complementar 8/IN01/DSIC/GSIPR (gestão de equipe de tratamento e resposta a incidentes em redes computacionais – ETIR: diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e nas entidades da Administração Pública federal), "o gerenciamento de incidentes de segurança em redes de computadores requer especial atenção da alta administração dos órgãos e das entidades da Administração Pública federal". E, conforme o item 4.8 da Norma Complementar 5/IN01/DSIC/GSIPR (criação de equipes de tratamento e resposta a incidentes em redes computacionais – ETIR), o tratamento de incidentes de segurança em redes computacionais é "o serviço que consiste em receber, filtrar, classificar e responder as solicitações e os alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e identificação de tendências".

APÊNDICE II
SUBPRÁTICAS

Quadro 2 – **Controles, medidas de segurança e subpráticas**

CONTROLE 1 – INVENTÁRIO E CONTROLE DE ATIVOS CORPORATIVOS
Medida de segurança 1.1 – Estabelecer e manter inventário detalhado de ativos corporativos
O inventário de ativos deve conter dados dos equipamentos de usuários finais, incluindo computadores portáteis e dispositivos móveis
O inventário de ativos deve incluir dados dos equipamentos, servidores e dispositivos de rede
O inventário de ativos deve incluir dados de dispositivos da internet das coisas (IoT)
O inventário deve incluir, para cada ativo, informações básicas – nome, endereços de rede, se estáticos, e *hardware* (MAC *address*), proprietário/responsável, local (dept., endereço) e indicação se aquele ativo tem permissão/aprovação ou não para se conectar à rede
A organização deve utilizar uma ferramenta de *Mobile Device Management* (MDM) para gerenciar os dispositivos móveis dos usuários finais
O inventário deve conter ativos conectados à infraestrutura da organização fisicamente, virtualmente e remotamente, incluindo aqueles em ambientes de nuvem (*cloud*)
O inventário deve incluir ativos conectados regularmente à infraestrutura de rede da organização, mesmo que não estejam sob seu controle
As informações constantes no inventário de ativos devem ser revisadas e atualizadas semestralmente ou ainda com mais frequência

Medida de segurança 1.2 – Tratar ativos não autorizados

O processo de tratamento dos ativos de *hardware* não autorizados deve ocorrer semanalmente ou ainda com mais frequência

Todo ativo de *hardware* não autorizado detectado deve ser removido da rede da organização

Todo ativo de *hardware* não autorizado, além de removido, deve ser impedido de se conectar à rede da organização em tentativas futuras

CONTROLE 2 – INVENTÁRIO E CONTROLE DE ATIVOS DE *SOFTWARE*

Medida de segurança 2.1 – Estabelecer e manter inventário de *software*

O inventário deve incluir informações básicas – título do *software*, empresa responsável (editor/*publisher*), data de instalação e propósito de negócio

Além das informações básicas, o inventário deve incluir informações adicionais sobre o *software*, tais como a URL de onde pode ser baixado, a indicação da(s) loja(s) de aplicativos, a versão, o respectivo mecanismo de implantação (*deployment*), a data de desativação etc.

As informações constantes no inventário de *software* devem ser revisadas e atualizadas semestralmente ou ainda com mais frequência

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

Usuários "comuns" devem ser impossibilitados de instalar qualquer *software* não autorizado nas máquinas da organização

Todo *software* autorizado e, portanto, suportado deve ser testado e homologado previamente pelo setor de TI da organização

Caso seja necessário instalar/executar algum *software* ainda não suportado, para atender os objetivos do negócio da organização, deve ser documentada uma exceção, justificando a necessidade, detalhando os controles mitigatórios eventualmente adotados e declarando a aceitação dos riscos residuais

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

Todo e qualquer *software* não suportado para o qual não tenha sido documentada uma exceção deve ser designado como não autorizado

O inventário de *software* deve ser revisado mensalmente, ou ainda com mais frequência, para detecção de *softwares* não suportados

Medida de segurança 2.3 – Tratar *softwares* não autorizados

O processo de tratamento de *softwares* não autorizados deve ocorrer mensalmente ou ainda com mais frequência

Sempre que for detectado um *software* não autorizado, deve ser documentada uma exceção, para autorizar seu uso, se necessário

Todo *software* não autorizado detectado que não justifique a documentação de uma exceção deve ser removido (desinstalado) do ativo

CONTROLE 7 – GESTÃO CONTÍNUA DE VULNERABILIDADES

Medida de segurança 7.1 – Estabelecer e manter processo de gestão de vulnerabilidades

O processo de gestão de vulnerabilidades deve ser documentado

O processo de gestão de vulnerabilidades deve ser formalmente aprovado

O processo de gestão de vulnerabilidades deve definir os diversos papéis e as responsabilidades associadas, incluindo as atividades de monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, a aplicação de correções, o acompanhamento dos ativos, o desempenho da função de coordenação e a documentação associada a essas atividades

O processo de gestão de vulnerabilidades deve ser revisado e atualizado anualmente ou ainda com mais frequência

Independentemente da revisão periódica, o processo de gestão de vulnerabilidades deve ser atualizado sempre que a organização passar por mudança significativa que possa impactá-lo

Medida de segurança 7.2 – Estabelecer e manter processo de correção de vulnerabilidades

O processo de correção de vulnerabilidades deve ser documentado

O processo de correção de vulnerabilidades deve ser formalmente aprovado

As correções das vulnerabilidades identificadas devem ser priorizadas, de acordo com os respectivos riscos, derivados de avaliações de probabilidade e impacto no negócio, por exemplo, para cada vulnerabilidade

As vulnerabilidades e seus respectivos riscos devem ser revisados mensalmente ou ainda com mais frequência

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

A organização deve monitorar constantemente fontes públicas e privadas de informações, para identificar ameaças e vulnerabilidades relacionadas a seus sistemas operacionais, bem como a existência de correções (*patches*) e/ou outras formas de mitigar os riscos associados

A organização deve utilizar ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos sistemas operacionais de seus ativos

As correções (*patches*) de sistemas operacionais devem ser testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão, sem trazer novos riscos e/ou causar efeitos adversos intoleráveis

A verificação da necessidade de atualização/aplicação de correções (*patches*) nos sistemas operacionais deve ocorrer mensalmente ou ainda com mais frequência

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

A organização deve monitorar constantemente fontes públicas e privadas de informações, para identificar ameaças e vulnerabilidades relacionadas a seus aplicativos/programas, bem como a existência de correções (*patches*) e/ou outras formas de mitigar os riscos associados

A organização deve utilizar uma ferramenta automatizada para realizar a gestão da aplicação de correções (*patches*) nos aplicativos (programas) de seus ativos

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

As correções (*patches*) de aplicativos (programas) devem ser testadas e avaliadas antes de serem instaladas, de modo a assegurar que efetivamente resolvam o problema em questão, sem trazer novos riscos e/ou causar efeitos adversos intoleráveis

A verificação da necessidade de atualização/aplicação de correções (*patches*) nos aplicativos (programas) deve ocorrer mensalmente ou ainda com mais frequência

CONTROLE 14 – CONSCIENTIZAÇÃO SOBRE SEGURANÇA E TREINAMENTO DE COMPETÊNCIAS

Medida de segurança 14.1 – Estabelecer e manter programa de conscientização em segurança

O programa de conscientização em segurança deve ser documentado

O programa de conscientização em segurança deve ser formalmente aprovado

Os colaboradores devem receber treinamento geral em segurança – saber como lidar com os ativos/dados corporativos de maneira segura, logo após sua contratação

Os colaboradores devem receber treinamento geral em segurança anualmente ou ainda com mais frequência

O programa de conscientização em segurança deve considerar os diferentes papéis desempenhados pelos colaboradores

Antes de assumir novas posições na organização, os colaboradores devem receber treinamento específico para os requisitos de segurança dos papéis a serem desempenhados

Medida de segurança 14.1 – Estabelecer e manter programa de conscientização em segurança
O conteúdo do programa de conscientização em segurança deve ser revisado e atualizado anualmente ou ainda com mais frequência
Independentemente da revisão periódica, o conteúdo do programa de conscientização em segurança deve ser atualizado sempre que a organização passar por mudança significativa que pode impactá-lo
Medida de segurança 14.2 – Treinar colaboradores para reconhecer ataques de engenharia social
O treinamento deve abordar ataques do tipo *phishing*
O treinamento deve abordar técnicas de pretexto (*pre-texting*)
O treinamento deve abordar técnicas de "isca"
O treinamento deve abordar ataques do tipo quiproquó (*quid pro quo*)
O treinamento deve abordar ataques do tipo "carona" (*tailgating*)
Medida de segurança 14.3 – Treinar colaboradores em melhores práticas de autenticação de usuários
O treinamento deve abordar dicas para composição de senhas seguras/fortes
O treinamento deve abordar aspectos relativos à guarda das senhas, incluindo ferramentas específicas de gerenciamento de credenciais
O treinamento deve abordar autenticação multifator – *multi-factor authentication* (MFA)

Medida de segurança 14.4 – Treinar colaboradores em melhores práticas de tratamento de dados
O treinamento deve abordar a política de mesa e tela limpas
A organização deve possuir política de classificação da informação formalmente aprovada, cujo conteúdo faça parte do escopo do treinamento
O treinamento deve abordar a proteção das informações contidas em ativos portáteis – *notebooks*, *tablets*, celulares, mídias removíveis, a exemplo do armazenamento apenas dos arquivos estritamente essenciais e da aplicação de mecanismos de proteção criptográfica
O treinamento deve abordar aspectos relacionados à deleção permanente de arquivos e dados (*data wiping*) e ao descarte seguro de mídias/equipamentos
Medida de segurança 14.5 – Treinar colaboradores para evitar exposição não intencional de dados
O treinamento deve abordar a adoção de cuidados gerais quanto à guarda e ao uso de equipamentos portáteis – *notebooks, tablets*, celulares, mídias removíveis
O treinamento deve abordar a conferência dos destinatários antes do envio de comunicações (*e-mails*) que contenham informações sensíveis
O treinamento deve abordar aspectos relacionados à publicação de conteúdos da organização em aplicativos de mensageria e/ou redes sociais
Medida de segurança 14.6 – Treinar colaboradores para reconhecer e notificar incidentes de segurança
O treinamento deve abordar os principais vetores de ataque – mídias removíveis, sítios/*e-mails* maliciosos, perda/furto de equipamentos – e como cada um pode ser explorado
O treinamento deve abordar sinais precursores e indicadores da ocorrência de incidentes

Medida de segurança 14.6 – Treinar colaboradores para reconhecer e notificar incidentes de segurança

Além de ensinar os colaboradores a reconhecer sinais de ocorrência de incidentes, o treinamento deve capacitá-los a identificar o tipo, a extensão e a magnitude do problema

Além de capacitar os colaboradores a reconhecer incidentes de segurança, o treinamento deve orientá-los quanto aos canais e meios apropriados para a respectiva notificação

Medida de segurança 14.7 – Treinar colaboradores para identificar e notificar falta de atualização de segurança nos ativos corporativos

O treinamento deve capacitar os colaboradores a verificar se as versões dos *softwares* e pacotes de correções (*patches*) instalados nos ativos corporativos estão desatualizadas

O treinamento deve ensinar os colaboradores a reconhecer a ocorrência de falhas na execução de processos/ferramentas automatizados – mensagens de erro, análise de *logs* etc.

O treinamento deve reforçar a necessidade de notificar o setor de TI sempre que alguma das ocorrências descritas nos itens anteriores for identificada

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

O treinamento deve abordar os riscos envolvidos na conexão a redes inseguras – captura de credenciais/senhas e comprometimento do ativo, a partir da instalação de um *malware*

O treinamento deve abordar os riscos envolvidos na transmissão de dados por meio de redes inseguras – vazamento ou adulteração dos dados e exposição de dados pessoais

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

O treinamento deve abordar a evolução histórica dos protocolos de criptografia de redes *wi-fi* (WEP, WPA e WPA2) e suas diferenças em termos da segurança das respectivas conexões

O treinamento deve capacitar os colaboradores que atuam em regime de trabalho remoto a configurar a infraestrutura de rede local, de modo a aumentar a segurança das conexões

CONTROLE 17 – GESTÃO DE RESPOSTAS A INCIDENTES

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

A organização deve designar responsável por gerenciar o processo de tratamento de incidentes – coordenar e documentar os esforços de resposta e recuperação

Além de um responsável principal, a organização deve designar, pelo menos, mais um substituto (*backup*), sendo que não podem se afastar simultaneamente

A equipe de tratamento de incidentes deve ser composta apenas por colaboradores da própria organização. Caso possua funcionários terceirizados, todo o trabalho realizado por eles deve ser supervisionado por, pelo menos, um colaborador da organização

As designações dos responsáveis devem ser revisadas anualmente ou ainda com mais frequência

Independentemente da revisão periódica, as designações dos responsáveis devem ser revisadas sempre que a organização passar por mudança significativa que possa impactar o processo de tratamento de incidentes

Medida de segurança 17.2 – Estabelecer e manter informações de contato para reporte de incidentes de segurança
A relação deve conter as informações de contato de todos os *stakeholders* que precisam ser informados, caso ocorra algum incidente de segurança – colaboradores internos, funcionários terceirizados, seguradoras, agentes da lei, agências/órgãos governamentais, CTIR Gov, CERT.br
A relação deve ser comunicada periodicamente aos colaboradores que dela farão uso, frisando suas responsabilidades e a obrigação de reportar incidentes de segurança às partes interessadas As informações de contato constantes na relação devem ser verificadas anualmente ou ainda com mais frequência, para garantir que estejam sempre atualizadas
Medida de segurança 17.3 – Estabelecer e manter processo para recebimento de notificação de incidentes
O processo deve estabelecer a responsabilidade e obrigação dos colaboradores de notificar qualquer evento de SegInfo do qual tomem ciência e especificar: (i) o prazo para realização da notificação; (ii) a quem a notificação deve ser encaminhada; (iii) como ela deve ser feita; e (iv) quais informações mínimas deve conter
O processo deve ser conhecido por todos e estar à disposição de todos os colaboradores da organização
O processo deve ser revisado anualmente ou ainda com mais frequência
Independentemente da revisão periódica, o processo deve ser revisado sempre que a organização passar por mudança significativa que possa impactá-lo

Fonte: CIS Controls® Version 8 (tradução e adaptação livres).

Responsabilidade pelo conteúdo
Secretaria de Fiscalização de Tecnologia da Informação (Sefti)
Diretoria de Fiscalização de Governança de TI - 2 (Digov-1)

Projeto gráfico, diagramação e capa
Secretaria de Comunicação (Secom)
Serviço de Criação e Editoração (Secrid)

Tribunal de Contas da União
SAFS Quadra 4 Lote 1
Edifício Sede
70.042-900, Brasília – DF
(61) 3527-7222

Ouvidoria do TCU
0800 644 1500
ouvidoria@tcu.gov.br

Impresso pela Senge/Segedam

Missão

Aprimorar a administração pública em benefício da sociedade por meio do controle externo.

Visão

Ser preferência na promoção de uma administração pública efetiva, ética, ágil e responsável.

www.tcu.gov.br