Relatório de Auditoria n. 1/2021

1. Introdução

Trata-se de relatório de auditoria realizada em conformidade com o Plano Anual de Controle Interno (Paci) de 2020 desta Secretaria, com foco na avaliação de aspectos de governança e de gestão do processo de trabalho de desenvolver e implementar níveis e estratégias de proteção de dados, segurança e privacidade.

2. O tema avaliado compõe a arquitetura de processos da Diretoria de Inovação e Tecnologia da Informação (Ditec), sendo resultado da união dos seguintes processos Cobit 5: APO 13 – Gerenciar Segurança e DSS 05 – Gerenciar Serviço de Segurança.

1.1. O ambiente de segurança da informação no cenário global

3. Segundo a Organização das Nações Unidas (ONU), mais da metade da população mundial possuía mecanismos de conexão online em 2018. Até o final daquele ano, 51,2% dos indivíduos, equivalente a 3,9 bilhões de pessoas, estavam usando a Internet. Esse é um passo significativo para uma sociedade da informação global mais inclusiva, mas traz também uma necessidade premente de maior proteção cibernética[1].

4. Por sua vez, relatório do Fórum Econômico Mundial[2] indica que a crescente interdependência cibernética das redes de infraestrutura em nível global é um dos principais fatores de risco, pois ataques computacionais, defeitos de softwares e outros fatores podem provocar falhas sistêmicas que se

[1] Disponível em: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf. Acesso em: 2 dez. 2020.
[2] Disponível em: http://www3.weforum.org/docs/GRR17_Report_web.pdf. Acesso em: 2 dez. 2020.

propagam pelas redes afetando a sociedade e as organizações, em particular, de maneiras imprevistas e altamente impactantes.

5. Nesse cenário de constante evolução digital, observa-se que os usuários demandam serviços inovadores que proporcionem, ao mesmo tempo, eficácia na segurança das informações e transparência na gestão da privacidade dos seus dados. Como exemplos dessas soluções, podem ser citados os aplicativos para dispositivos móveis, a incorporação de estratégias de *data analytics* para tomada de decisão e o uso massivo de *internet-of-things* (IoT).

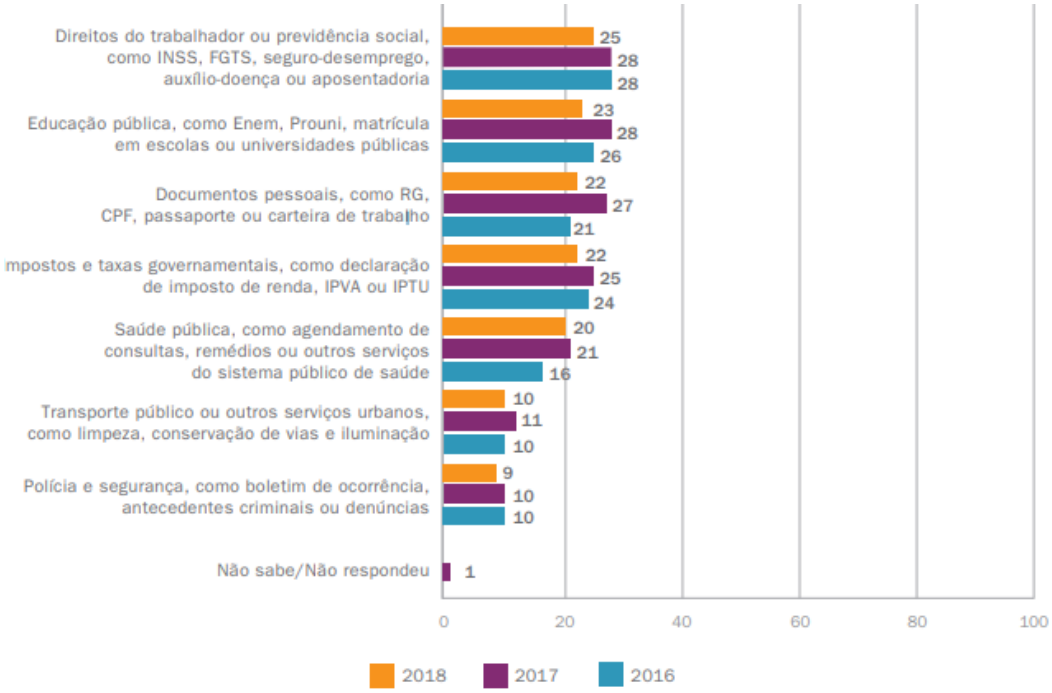
6. Naturalmente, à medida que novas tecnologias são desenvolvidas, surgem novos riscos inerentes a essas soluções, que precisam ser reavaliados continuamente. Logo, o monitoramento dos riscos cibernéticos torna-se um processo relevante para a governança organizacional com foco na resiliência aos eventos de maior impacto, especialmente aqueles com consequências negativamente disruptivas.

1.2. O ambiente de segurança da informação no cenário nacional

7. De acordo com a pesquisa TIC Domicílios, realizada em 2019 pelo Cetic.br, departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ligado ao Comitê Gestor da Internet no Brasil (CGI.br), cerca de 127 milhões de brasileiros acessaram regularmente a Internet, o que representa 70% da população[3]. Essa pesquisa é realizada anualmente desde 2005, com o objetivo de mapear o acesso às TIC nos domicílios urbanos e rurais do país. O Gráfico 1 mostra os serviços públicos mais procurados ou realizados entre 2016 e 2018, em percentual de usuários.

[3] Disponível em: https://cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf. Acesso em: 2 dez. 2020.

Gráfico 1 - Serviços públicos mais procurados ou realizados entre 2016 e 2018



Fonte: CERT.br[4] (2020).

8. Com base nisso, verifica-se uma demanda por canais de atendimento dos mais variados serviços públicos, principalmente aqueles relativos às áreas trabalhista, educacional, tributária, saúde e segurança pública[5].

9. Assim, com o objetivo de mitigar os riscos ligados à segurança da informação, o Poder Executivo Federal normatizou a Estratégia Nacional de Segurança Cibernética[6], entre outras iniciativas. Nesse cenário, os aspectos

[4] Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 2 dez. 2020.

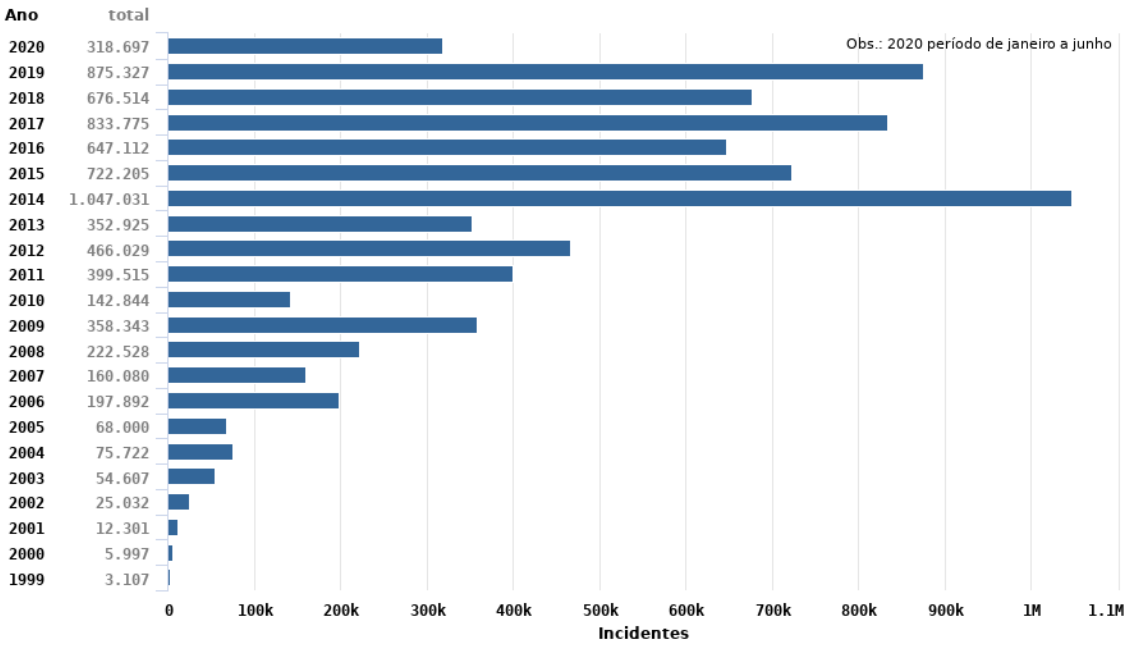
[5] Os dados relativos à Pesquisa TIC Domicílios realizada em 2019 não permitiram uma comparação detalhada. Disponível em: https://cetic.br/media/docs/publicacoes/2/20201123121817/tic_dom_2019_livro_eletronico.pdf. Acesso em: 26 fev. 2020.

[6] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 2 dez. 2020.

ligados ao tema vêm ganhando notável importância, seja para cidadãos, seja para as instituições.

10. O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[7], por sua vez, é mantido pelo Núcleo de informação e Coordenação do Ponto BR (NIC.br), do Comitê Gestor da Internet no Brasil (CGI.br). Trata-se de um ponto central responsável por mapear os incidentes de segurança no país, provendo também a coordenação no processo de respostas a esses eventos. O Gráfico 2 mostra o total absoluto de incidentes anualmente reportados no Brasil ao CERT.br.

Gráfico 2 - Total de incidentes no Brasil reportados ao CERT.br
de janeiro de 1999 a junho de 2020



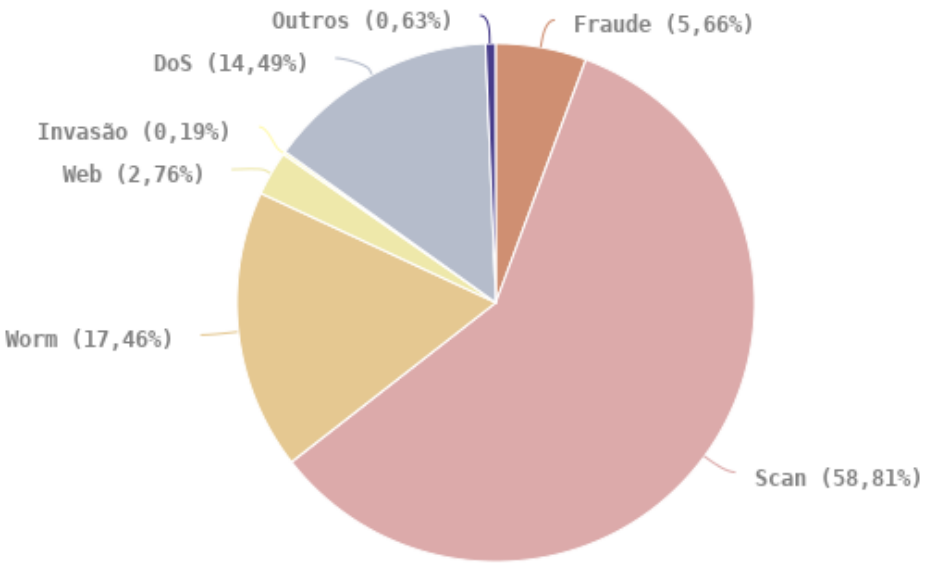
Fonte: CERT.br[8] (2020).

11. De modo geral, mesmo com variações em anos específicos, verifica-se uma tendência de aumento dos incidentes reportados à organização, com um pico em 2014.

[7] Disponível em: https://www.cert.br/sobre/. Acesso em: 2 dez. 2020.
[8] Disponível em: https://www.cert.br/stats/incidentes/. Acesso em: 2 dez. 2020.

12. O Gráfico 3 especifica os incidentes relativos à segurança da informação reportados no ano de 2020.

Gráfico 3 - Tipo de ataques entre janeiro a junho de 2020 no Brasil[9]



Fonte: CERT.br (2020)[10].

13. Vê-se que o ataque cibernético mais comum no Brasil é o *scan*, que pode ser definido como uma técnica de exploração das vulnerabilidades de um alvo

[9] Legenda:

- **worm**: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.
- **dos** (DoS -- *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.
- **invasão**: um ataque bem sucedido que resulte no acesso não autorizado a um computador ou rede.
- **web**: um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.
- **scan**: notificações de varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
- **fraude**: segundo Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com intuito de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.
- **outros**: notificações de incidentes que não se enquadram nas categorias anteriores.

[10] Disponível em: https://www.cert.br/stats/incidentes/2020-jan-jun/tipos-ataque.html. Acesso em: 2 dez. 2020.

em potencial que antecede os demais ataques. Em segundo lugar, verifica-se o ataque por *worms,* com sua propagação automática peculiar e, em terceiro, o ataque de negação de serviço (DoS) que se concentra na indisponibilidade dos ativos.

14. Com o advento da pandemia de Covid-19, houve ainda um aumento do nível de risco cibernético em escala global, devido à disponibilização dos serviços por meio de acesso remoto aos ativos de TIC que, antes, estavam disponíveis majoritariamente para consumo interno nas organizações. A título de exemplos, alguns órgãos públicos foram recentemente alvos de ataques, como o Superior Tribunal de Justiça[11], o Tribunal Superior Eleitoral[12], e o Tribunal Regional da 1ª Região[13], com foco, principalmente, em atingir a disponibilidade dos respectivos serviços. Assim, a concretização desses riscos relativos à segurança da informação em órgãos públicos federais reforça a tempestividade desta ação de controle, ao mesmo tempo em que corrobora a relevância do tema para a administração pública.

15. Em compensação, do ponto de vista normativo, existem importantes institutos criados para regulamentar as ações no ambiente cibernético. Cite-se, inicialmente, o Marco Civil da Internet, que foi instituído pela Lei n° 12.965/2014[14], regulando o uso da Internet no Brasil por meio da previsão de princípios, garantias, direito e deveres, e determinando diretrizes para a atuação do Estado.

---

[11] Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/06112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 2 dez. 2020.

[12] Disponível em: https://www.tse.jus.br/imprensa/noticias-tse/2020/Novembro/tentativas-de-ataques-de-hackers-ao-sistema-do-tse-nao-afetaram-resultados-das-eleicoes-afirma-barroso. Acesso em: 2 dez. 2020.

[13] Disponível em: https://www.cjf.jus.br/cjf/noticias/2020/11-novembro/nota-esclarecimento-trf1-acesso-indevido. Acesso em: 2 dez. 2020.

[14] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 2 dez. 2020.

16. Mais recentemente, foi promulgada a Lei Geral de Proteção de Dados Pessoais, lei nº 13.709/2018[15], que regula as atividades de tratamento de dados pessoais e altera alguns dispositivos do Marco Civil da Internet.

17. No ano de 2020, foi publicada a Estratégia Nacional de Segurança Cibernética, formalizada por meio do Decreto n. 10.222/2020[16], aprovando a estratégia para o quadriênio 2020-2023. Esse normativo apresenta uma série de ações ligadas à segurança da informação, tais como: fortalecimento das ações de governança cibernética, estabelecimento de um modelo centralizado de gestão em âmbito nacional e elevação do nível de proteção do governo.

2. Abordagem da auditoria

18. O objeto desta ação de controle foi selecionado por meio de avaliações dos itens que compõem a arquitetura de processos da área de TIC. Essas apreciações foram realizadas pelos servidores do Nuati e da Ditec, aferindo os critérios de maturidade e de relevância de cada processo, equitativamente, por seus respectivos membros.

19. Em seguida, os riscos de cada um dos processos foram analisados seguindo os critérios da metodologia corporativa de gestão de riscos[17], a fim de mensurar a probabilidade e o impacto dos seus eventos adversos. Como resultado desse trabalho, os seguintes riscos foram elencados:

a. plano de segurança não ser operacional, ou não atingir os objetivos pretendidos;

b. informações críticas para os negócios não estarem disponíveis;

c. incapacidade de recrutar o pessoal adequado.

---

[15] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 2 dez. 2020.
[16] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em: 2 dez. 2020.
[17] Disponível em: https://www2.camara.leg.br/a-camara/estruturaadm/gestao-na-camara-dos-deputados/governanca/documentos/metodologia-corporativa-de-gestao-de-riscos . Acesso em: 2 dez. 2020.

20. Dentre as diversas espécies de ações de controle previstas no Estatuto de Controle Interno[18], o Nuati optou por adotar a avaliação da adequação do gerenciamento corporativo de riscos, baseando-se nas boas práticas recomendadas por instituições como o Instituto de Auditores Internos (IIA)[19] e o Tribunal de Contas da União (TCU)[20]. Ao empregar esse tipo de auditoria, os seguintes riscos foram acrescentados ao escopo dos trabalhos:

a. os objetivos do processo não suportarem ou não estarem alinhados com a missão da Casa;

b. os riscos significativos do processo não serem identificados e avaliados;

c. as respostas aos riscos não serem selecionadas de forma a manter o alinhamento com o apetite de risco da Ditec e da Casa; e

d. as informações quanto aos riscos relevantes não serem capturadas e comunicadas de forma oportuna, impedindo que a administração cumpra com suas responsabilidades.

21. Vale destacar que o processo Cobit DSS 05 – Gerir serviços de segurança foi objeto do Relatório de Auditoria n. 1/2015-Nuati/Secin, em que foram avaliadas as seguintes práticas de gestão: proteção contra *malware*; gerenciamento da segurança de rede e de conectividade; gerenciamento da segurança de *endpoints*; gerenciamento da identidade e o acesso lógico dos usuários; gerenciamento do acesso físico a instalações de TI; gerenciamento de documentos sensíveis e dispositivos de saída; e monitoramento da infraestrutura para eventos relacionados à segurança.

---

[18] Estatuto de Controle Interno, Secretaria de Controle Interno, Câmara dos Deputados, p. 14. Disponível em: http://bd.camara.gov.br/bd/bitstream/handle/bdcamara/35419/estatuto_controle_interno.pdf. Acesso em: 31 jul. 2019.

[19] Disponível em: https://iiabrasil.org.br/korbilload/upl/ippf/downloads/declarao-de-pos-ippf-00000001-21052018101250.pdf. Acesso em: 2 dez. 2020.

[20] Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F6364D8370163B1929CD82D2B. Acesso em: 2 dez. 2020.

22. O escopo dos trabalhos da atual ação foi delimitado pela avaliação dos riscos relacionados à governança e à gestão dos seguintes processos e atividades da área administrativa desta Casa: escolha da solução de acesso remoto por parte dos servidores da Casa em regime de teletrabalho, avaliação do Plano de Ação em Segurança da Informação (PASI) e descentralização de TI.

3. Boas práticas administrativas observadas

23. No decorrer da auditoria, durante a avaliação dos controles internos administrativos, foram identificadas boas práticas de gestão, que efetivamente contribuem para a mitigação de alguns riscos:

a. reuniões do Comitê Gestor de Segurança da Informação (CGSI)[21] e do Comitê de Gestão Estratégica (CGE)[22] demonstrando a importância da governança e da gestão da segurança da informação percebida pela alta administração da Casa;

b. normatização dos procedimentos e regras para fins de prevenção à infecção e à propagação do covid-19 no âmbito da Câmara dos Deputados, com emprego de teletrabalho[23];

c. normatização das atribuições e responsabilidades sobre soluções de Tecnologia da Informação e Comunicação (TIC)[24].

4. Pontos de auditoria

4.1. Ausência de diretrizes básicas de construção de soluções de TIC para a Casa

[21] Disponível em: https://camaranet.camara.leg.br/web/gestao-estrategica/atas. Acesso em: 2 dez. 2020.
[22] Disponível em: https://camaranet.camara.leg.br/web/gestao-estrategica/gestao-estrategica/governanca-da-gestao-estrategica/atas. Acesso em: 2 dez. 2020.
[23] Disponível em: https://www2.camara.leg.br/legin/int/atomes/2020/atodamesa-118-11-marco-2020-789835-publicacaooriginal-160111-cd-mesa.html. Acesso em: 2 dez. 2020.
[24] Disponível em: https://www2.camara.leg.br/legin/int/portar/2019/portaria-88-29-marco-2019-788837-publicacaooriginal-158741-cd-dg.html. Acesso em: 2 dez. 2020.

4.1.1. Situação encontrada

24. A ausência de normatização para regulamentar as diretrizes básicas de TIC refletiu em deficiências nos controles e no monitoramento, acarretando em vulnerabilidades, tais como as destacadas no Relatório de Auditoria Conjunta n. 1 de 2020, processo eDoc 430140/2020, que demonstrou a inobservância da Política de Segurança da Informação (PSI) pela unidade de TI do Pró-Saúde.

4.1.2. Critérios

a) Política de Segurança da Informação, artigo 4º, incisos VII, VIII; artigo 5º, inciso IV; artigo 6º, inciso I (Ato da Mesa n. 47, de 16/7/2012);

b) Ato de criação da Diretoria de Inovação e Tecnologia da Informação da Câmara dos Deputados, Anexo VI,1,c (Ato da Mesa n. 215, 6/12/2017);

c) Cobit 5 – processo APO 13 (Gerenciamento da segurança);

d) Cobit – processo DSS 05 (Gerenciamento dos serviços de segurança);

e) Planejamento Estratégico 2012-2023 - Linha de atuação 7.3;

f) Norma ABNT NBR ISO/IEC 27005:2019 (Gestão de riscos de segurança da informação);

g) Norma ABNT NBR ISO/IEC 27001:2013 (Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos).

4.1.3. Evidências

a) Não foram identificadas diretrizes básicas vigentes sobre a prestação de serviços de TIC, de forma descentralizada, a exemplo da Decisão Ceti n. 1/2013, expirada em 2017;

b) Testes substantivos realizados na base de dados, em ambiente de produção, do Sistema de Gestão do Pró-Saúde, registrados no Relatório de Auditoria Conjunta n. 1/2020 - Secin, que tramita na Casa no processo edoc n. 430140/2020.

4.1.4. Causa

a) Ausência de controles e diretrizes formalizados para a construção de soluções de TI de forma descentralizada nas unidades administrativas, observando as políticas, regras e padrões institucionais.

4.1.5. Efeitos potenciais

a) Arquitetura de informação fragilizada;
b) Vazamento de informações;
c) Danos à imagem institucional;
d) Prejuízos financeiros.

4.1.6. Esclarecimentos do auditado

25. A equipe de auditoria questionou a gestão acerca da existência de normativo vigente que vincule as unidades descentralizadas de TIC aos padrões de segurança da informação normatizados e adotados pela Ditec. Em resposta, foram encaminhadas manifestações separadamente por algumas das principais unidades envolvidas, a saber: Ditec, Diretoria-Geral e Cedi.

26. A princípio, a Ditec explanou:

> Não existe normativo vigente para tal finalidade. A Ditec entende que as atividades especializadas e estruturantes de TI devem ser conduzidas e executadas pela área técnica de TI da instituição, de forma centralizada.
>
> Mesma lógica tem sido desenvolvida pelas instituições que optaram por uma transformação digital na qual os processos são plenamente digitalizados de forma integrada com sustentabilidade e economia de recursos (humanos e financeiros). Nesse cenário, as organizações têm investido fortemente na mudança de cultura da corporação na qual as pessoas são capacitadas a usar recursos digitais com maior profundidade e amplitude do que fazem hoje. Passam ser capazes de gerar gráficos, preparar relatórios, comparar dados com várias ferramentas de usuários mais elaboradas.
>
> Como consequência, a área de TI pode atender a um grande número de serviços digitais (processos digitalizados e/ou automatizados) construídos em visão sistêmica, com integração e reaproveitamento de vários componentes. Nesse novo

> patamar de serviços digitais, é de extrema relevância a existência de experientes projetistas e arquitetos digitais e profissionais de elevado nível de conhecimento em diferentes modelos tecnológicos que evoluem no mercado mundial diariamente. À complexidade das tecnologias são acrescidos diferentes modelos de comercialização e manutenção, amplificando profissionais de alta qualificação e constante aprendizagem.
>
> No que se refere aos dados, nesse novo modelo, a área de TI realiza uma gestão completa nos dados, viabilizando qualidade, segurança e integridade em todos os processos. Esse ecossistema de dados é organizado em estruturas disponibilizadas para que os demais colaboradores da organização, diante de uma nova cultura digital, possam construir painéis e relatórios de baixa e média complexidade, reservando à área de TI, os painéis mais complexos.
>
> Convém o registro de que a movimentação do pessoal especializado da Ditec para outras unidades organizacionais diminui a capacidade desta diretoria em prover soluções digitais integradas e modernas que exigem recursos profissionais com a formação específica. Adicionalmente, a existência de núcleos de TI amplia as linhas paralelas de digitalização, concorrendo com à estratégia de transformação digital e a visão sistêmica do complexo digital de uma organização.

27. A Diretoria-Geral, por seu turno, destacou que o Ato da Mesa nº 47/2012, que dispõe sobre a política de segurança da informação na Câmara dos Deputados, é atualmente o normativo que direciona as ações relativas ao tema na Casa, cujas diretrizes alcançam todos os servidores e núcleos de TI. Por consequência, independentemente de sua disposição centralizada ou descentralizada, o desempenho das atividades de TIC deve estar alinhado à Unidade Central. Nesse sentido, a DG entende que a resposta da Ditec informando a inexistência de normativo vigente para tal finalidade, refere-se a uma norma específica para núcleos descentralizados de TI, que, embora existentes, não refletem um modelo adotado oficialmente pela Administração.

28. Finalmente, o Cedi relatou:

> Informamos que não conhecemos nenhum normativo específico acerca de orientações de segurança voltado particularmente para os núcleos descentralizados de TI. De todo modo, conforme previsto na política de segurança da informação (Ato da Mesa 47/2012), em seu artigo 11, II ("Art. 11. São

> atribuições das unidades administrativas da Câmara dos Deputados: (...) II - zelar pela segurança da informação no âmbito dos processos de trabalho e atividades sob sua responsabilidade;"), o Núcleo de Tecnologia do Cedi tem buscado adotar rotinas de segurança em tecnologia compatíveis com os processos de trabalho e atividades tratadas no escopo dos sistemas de informática desenvolvidos internamente, sempre em contato direto e com o apoio da Ditec. São ações que tem a finalidade de buscar sempre manter em alto nível os requisitos de confidencialidade, integridade e disponibilidade dos dados geridos pelos sistemas internos aos Cedi desenvolvidos pelo NUTEC. Por exemplo, a autenticação de nossos sistemas internos é realizada por integração à solução corporativa disponibilizada pela DITEC, o CAS (Central Authentication Service) da RedeCamara, mesmo quando o acesso é feito pela Web (mudança que aconteceu com a definição de trabalho remoto). Além disso, dentro dos sistemas há outras rotinas de segurança, implementadas tanto no *backend* quanto no *frontend* das aplicações. Também existem rotinas de backups periódicas aplicadas aos sistemas e às bases de dados, bem como separação entre os ambientes de desenvolvimento e de produção.
>
> Retornando ao questionamento apresentado ("i. existe normativo vigente que vincule as unidades descentralizadas de TIC aos padrões de segurança da informação normatizados e adotados pela Ditec?") entendemos ser importante o desenvolvimento de normativo que vincule/oriente ações de segurança em tecnologia de ordem mais gerais, e que haja em tal norma também a previsão de mecanismos de apoio técnico efetivos para a implementação e suporte dessas ações. Cabe, por fim, ressaltar o bom contato que temos recebido da área técnica da Ditec nas soluções de questões relacionadas ao tema. Facilitar esse tipo de entrosamento é importante para ações efetivas e integradas de segurança das soluções tecnológicas.

4.1.7. Análise

29. Preliminarmente, cabe realçar o empenho da gestão em estimular a inovação em nível organizacional a fim de aprimorar continuamente a qualidade dos serviços na Casa, como pode ser observado, por exemplo, no projeto de Transformação Digital proposto recentemente pela Ditec. Nesse contexto, a segurança da informação é considerada uma aliada a fim de garantir a eficiência dos serviços tecnológicos.

30. Por outro lado, conforme o Relatório de Auditoria Conjunta n. 1/2020 – Secin, a concretização da vulnerabilidade no gerenciamento de perfis de acesso

do Sistema de Gestão do Pró-Saúde, permitindo privilégio de consulta e modificação dos dados em ambiente de produção, em uma unidade administrativa responsável por serviços de alta criticidade, corrobora a necessidade de uma regulamentação que estabeleça diretrizes em um modelo distribuído de prestação de serviços tecnológicos.

31. Há um risco de que soluções sejam desenvolvidas por essas unidades descentralizadas sem a observância das políticas, regras e padrões institucionais, tais como a Política de Segurança da Informação. Considera-se que esses parâmetros institucionais são essenciais, pois atendem ao princípio da gestão sistêmica da segurança da informação, previsto na PSI, Art. 4º, VII.

32. De fato, já houve previsão de um modelo híbrido, conforme Decisão do Ceti n. 1/2013, com unidades administrativas com equipes de TIC setoriais com a missão de desenvolver soluções tecnológicas locais, nos seguintes termos:

> 2. A Câmara dos Deputados adotará modelo de prestação de serviços híbrido composto por uma área responsável pela TIC e com a utilização de outros recursos humanos especializados distribuídos nas demais unidades administrativas da Casa.
> a. As atividades de TIC devem estar em conformidade com as políticas, regras e padrões estabelecidos pela Área Responsável pela TIC, bem como com a Política de Gestão de Conteúdos Informacionais, a Política de Segurança da Informação, a Arquitetura de Negócios e Informação e o modelo de Governança de TIC da Câmara dos Deputados, em especial o Plano Estratégico de TIC (Peti) e o Plano Diretor de TIC (PDTI).

33. Entretanto, esse normativo expirou em 2017 e, até o presente momento, não foi identificado outro instituto que regulamente tais diretrizes básicas em um modelo tecnológico distribuído.

34. Nesse sentido, ao longo da pretendida transformação digital, observa-se a necessidade de mitigação dos riscos presentes, por meio de controles adequados, para que seja possível a disponibilização de soluções descentralizadas que atendam aos mesmos níveis de segurança da informação utilizados pela própria Ditec.

35. Os objetivos definidos na PSI reiteram a necessidade de uma visão corporativa do tema:

> Art. 5º Com vistas à observância aos princípios descritos no artigo 4º, esta Política está voltada aos seguintes objetivos:
> I - instituir uma cultura organizacional aderente à segurança da informação, compreendendo ações destinadas a fomentar entre os usuários a constante observância quanto às práticas destinadas à preservação dessa segurança;
> II - implantar a contínua avaliação dos riscos a que a informação está sujeita;
> III - estabelecer mecanismos que visem garantir a segurança da informação, em especial a confidencialidade, a integridade, a disponibilidade e a autenticidade nos projetos, processos e atividades da Câmara dos Deputados; e
> IV - implementar a governança da segurança da informação.

36. Vale ressaltar que a mitigação de riscos por meio de um ambiente de controle em um modelo híbrido de prestação de serviços é fundamental para que as unidades administrativas da Casa continuem entregando serviços inovadores e, ao mesmo tempo, observando os requisitos mínimos de confidencialidade, integridade e disponibilidade das informações.

37. Conforme estabelece o ato de transformação do então Centro de Informática em Ditec (Ato da Mesa n. 215/2017)[25], anexo VI, 1, c, é uma competência dessa Diretoria: “Planejar, coordenar controlar e orientar os órgãos departamentais que a compõem, supervisionando as atividades relacionadas à Tecnologia da Informação na Câmara dos Deputados”.

38. Assim, considerando que já existem efetivamente unidades descentralizadas, desenvolvendo e mantendo sistemas em plena produção, a mitigação que se vislumbra mais efetiva seria a definição de um conjunto de regras a serem observadas por tais unidades, garantindo o padrão de segurança desejado, alicerçado na PSI.

[25] Disponível em: https://www2.camara.leg.br/legin/int/atomes/2017/atodamesa-215-6-dezembro-2017-786039-anexo-cd-mesa.pdf. Acesso em: 2 dez. 2020.

4.1.8. Recomendações

a) Recomendar à Diretoria-Geral, na qualidade de unidade coordenadora do Comitê de Gestão Estratégica (CGE)[26], que elabore normativo estabelecendo as diretrizes mínimas para as soluções desenvolvidas por unidades de TIC descentralizadas, permitindo melhor controle das políticas, regras e padrões institucionais relativos, entre outros temas, à segurança da informação.
Prazo: 180 dias.

4.2. As responsabilidades para execução das ações de segurança da informação não estão bem definidas

4.2.1. Situação encontrada

39. As responsabilidades do CGSI possuem natureza deliberativa, sem apresentar atribuições de execução, o que pode dificultar as entregas previstas. Um exemplo disso é o não cumprimento integral das diversas ações previstas no Plano de Ação em Segurança da Informação (PASI) elaborado em 2014.

40. Por outro lado, as atribuições das áreas técnicas da Ditec resumem-se aos aspectos da segurança da informação no ambiente digital, que não engloba todo o universo de ações necessárias para a segurança da informação em nível institucional.

4.2.2. Critérios

a) Política de Segurança da Informação, Artigo 8º, § 3º, incisos I a IX (Ato da Mesa n. 47, de 16/7/2012);
b) Plano de Ação em Segurança da Informação 2014;
c) Cobit 5 - APO 13 (Gerenciamento da segurança);

[26] Ato da Mesa n. 245, de 2018, art. 2º.

d) Cobit – DSS 05 (Gerenciamento dos serviços de segurança);
e) Norma ABNT NBR ISO/IEC 27005:2011 (Gestão de riscos de segurança da informação);
f) Portaria de instalação e de funcionamento do CGSI, Artigo 3º (Portaria n. 407, de 30/09/2013).

4.2.3. Evidências

a) Atas das reuniões do CGSI;
b) Ata da reunião realizada no âmbito da auditoria em curso, entre o Nuati e a Ditec em 29/09/2020;
c) Ata da reunião realizada no âmbito da auditoria, entre o Nuati e o Cedi em 8/10/2020;
d) Política de Segurança da Informação, Artigo 8º, § 3º, incisos I a IX (Ato da Mesa n. 47, de 16/7/2012);
e) Portaria de instalação e de funcionamento do CGSI, Artigo 3º (Portaria n. 407, de 30/09/2013).

4.2.4. Causas

a) Aspectos da governança corporativa, relacionados à Segurança da Informação, incipientes;
b) Deficiências no controle e no acompanhamento da execução das ações priorizadas no CGSI.

4.2.5. Efeitos potenciais

a) Atraso nas entregas;
b) Desmotivação da equipe;
c) Ineficiência processual;
d) Riscos de confidencialidade, disponibilidade e integridade das informações cujas ações previstas não foram implementadas.

4.2.6. Esclarecimentos do auditado

41. Os auditores questionaram a gestão acerca da previsão de revisões periódicas das ações do PASI e quais seriam as unidades responsáveis pelas ações de Segurança da Informação, definidas pelo CGSI.

42. No tocante à previsão de revisões periódicas das ações do PASI, a Ditec informou que na época de lançamento do Plano, em 2014, não havia previsão para revisá-lo. Desta forma, passados seis anos, e considerando o nível de inovação e evolução a que os ambientes interno e externo relacionados à área de TIC estão sujeitos, sugere-se a atualização do plano, tornando-o mais aderente à nova realidade, e que mais alinhado à estratégia de transformação digital da Câmara dos Deputados.

43. A Ditec destacou que não há uma definição clara sobre quais unidades deveriam executar as ações de segurança da informação deliberadas no CGSI. A percepção é de que o Comitê foi criado para uma atuação eminentemente deliberativa. Ademais, percebe-se que há dificuldade para condução de determinadas ações que exigem um acompanhamento mais intensivo e cotidiano, uma vez que falta ao Comitê, por ser órgão com papel deliberativo, capacidade operacional para:

> 1) monitorar e responder de maneira mais rápida e efetiva aos desafios impostos por um cenário mundial cada vez mais dinâmico e desafiador;
>
> 2) lidar com grande volume de questões relacionadas com a segurança da informação no contexto corporativo, que exigem acompanhamento e coordenação entre diferentes atores;
>
> 3) desenvolver e aprofundar o conhecimento técnico em segurança da informação; e
>
> 4) implantar e gerir um Sistema de Gestão de Segurança da Informação (SGSI), que englobaria as estratégias, planos, políticas, medidas, controles, e diversos instrumentos voltados a estabelecer, implementar,

operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

44. A Diretoria-Geral, por sua vez, destacou que, em relação à previsão de revisões periódicas das ações do PASI, o Ato da Mesa n. 47/2012, que cria o Comitê Gestor de Segurança da Informação na Câmara dos Deputados, dispõe que as revisões da política de segurança da informação devem acontecer periodicamente no âmbito do Comitê, com encaminhamento para deliberação da autoridade competente, no caso, o CGE, conforme o disposto nos incisos I e IV do §3º do art. 8º.

45. A revisão, portanto, pode acontecer a qualquer tempo, e considera-se oportuno trazer o PASI à atual realidade, considerando as ações de transformação digital referenciadas pela Ditec.

46. Sobre quais unidades deveriam executar as ações de Segurança da Informação, a Diretoria-Geral informou que, após aprovadas pelo Comitê de Gestão Estratégica, deveriam ser executadas pelas unidades técnicas da Casa, a depender do processo de trabalho relacionado. A DG informou ainda que a solução apresentada pela Ditec parece direcionar as ações de segurança da informação para uma unidade administrativa dedicada ao tema, existente ou a ser criada. Tal solução não pode prescindir de uma análise conjunta com a área de recursos humanos, ponderando-se fatores positivos e negativos da atuação ou criação de um órgão de controle, ou de se trabalhar a cultura organizacional voltada aos valores e práticas relacionados à segurança da informação. Sobre o caráter deliberativo do Comitê, reforça-se a aplicação do art. 8º, § 3º, IV, do Ato da Mesa nº 47/2012, pelo qual o CGSI deve submeter suas deliberações à autoridade competente, que, por sua vez, poderá designar uma unidade técnica operacional para atender à questão.

47. Por fim, o Cedi informou que a previsão de revisão das ações do PASI deve ser respondida pelo coordenador do CGSI.

48. Sobre quais unidades deveriam executar as ações de Segurança da Informação, o Cedi informou que há necessidade de avaliar as competências normativas de cada uma das áreas. Em princípio, cabem à Ditec as análises quanto à segurança tecnológica em ambientes digitais, ao Depol e ao Detec as questões relacionadas à segurança de ambientes e estruturas físicas, bem como das pessoas, e ao Cedi observar os requisitos de segurança vinculados à autenticidade e preservação de informações arquivísticas e bibliográficas e, por meio da Coordenação de Preservação de Conteúdos Informacionais (Cobec), dos demais acervos informacionais da Casa. A análise das competências estabeleceria outras responsabilidades. De toda sorte, caberia à Diretoria-Geral coordenar a execução do Plano de Ação de Segurança da Informação. O CGSI seria, então, uma unidade de consultoria e especialização na análise, identificação de requisitos e relatoria da situação identificada.

4.2.7. Análise

49. A princípio, percebe-se a relevância do CGSI para a governança e gestão da segurança da informação quando suas competências foram destacadas na própria Política de Segurança da Informação, a saber:

> § 3º Compete ao Comitê Gestor de Segurança da Informação:
> I - avaliar periodicamente e manter atualizadas a política de segurança da informação e as normas dela decorrentes;
> II - demandar às unidades administrativas a elaboração de normas específicas relacionadas à segurança da informação em suas áreas de competência;
> III - receber, avaliar e validar propostas de normas relativas à segurança da informação;
> IV - encaminhar à autoridade competente para deliberação as propostas de atualização da política de segurança da informação e as propostas de normas correlatas;
> V - coordenar a implantação e atualização do SGSI a ser adotado pela Casa;
> VI - acompanhar e avaliar o sistema implantado conforme o inciso anterior;
> VII - coordenar a seleção, implantação e atualização da metodologia de análise periódica de riscos a ser adotada pela Casa, bem como a definição do escopo e abrangência dessas análises;

> VIII - planejar e coordenar ações institucionais de segurança da informação;
> IX - propor a inclusão das iniciativas relacionadas à segurança da informação no Plano Plurianual de Gestão de Conteúdos Informacionais e em suas atualizações.

50. Verifica-se, contudo, que as atribuições do Comitê possuem ênfase na coordenação e gestão das iniciativas organizacionais em segurança da informação. Não há previsão de competências operacionais, tampouco a existência de um quadro de servidores com atribuições prioritárias a fim de concretizar tais iniciativas, especialmente em tempos de carência por recursos humanos.

51. Por vezes, as ações priorizadas são executadas pelos mesmos servidores que compõem o CGSI, quando atuam nas áreas técnicas de origem, concomitantemente com as demais atividades, mas sem possuir uma priorização formal com a mesma eficácia que se observa, por exemplo, nos projetos corporativos. A Portaria n. 407[27], de 30/9/2013, da Diretoria-Geral, que dispõe sobre a instalação e o funcionamento do CGSI, estabelece atribuições para a Câmara Técnica, prevista pelo Ato da Mesa n. 47, de 2012, mas esta possuiria competências de assessoramento.

52. A Ditec possui unidades que atuam com atividades relacionadas à segurança da informação, mas suas atribuições são restritas aos aspectos técnicos da segurança cibernética, não abrangendo todas as responsabilidades inerentes à operacionalização da segurança da informação a nível institucional, como a elaboração de campanhas, levantamento de ativos de informação e identificação de vulnerabilidades no acesso físico a documentos, dentre outras ações.

53. Por meio de reuniões realizadas com as áreas da Ditec e Cedi, verificou-se que há uma percepção em comum de que existe a necessidade de uma maior

[27] Disponível em: https://www2.camara.leg.br/legin/int/portar/2013/portaria-407-30-setembro-2013-777183-publicacaooriginal-141365-cd-dg.html. Acesso em: 2 dez. 2020.

priorização das ações do CGSI, bem como da existência de estruturas capazes de operacionaliza-las.

54. Constatou-se que foram planejadas cinco ações principais para o PASI elaborado em 2014, mas que não foram finalizadas em sua completude até o presente momento. Dentre essas ações pendentes, destacam-se a implantação de um Sistema de Gestão de Riscos e do Inventário Informacional, que, caso tivessem sido integralmente realizados, permitiriam ao CGSI um ambiente mais favorável ao desempenho de suas atividades[28], refletindo uma melhoria na sua maturidade processual.

55. Além disso, surgiram novas atividades, como as discussões sobre a utilização de serviços de computação em nuvem e sobre a Lei Geral de Proteção de Dados (LGPD, Lei n. 13.709, de 2018), que também foram priorizadas nesse período.

56. Detectou-se ainda uma necessidade de revisar e atualizar as ações do PASI devido às mudanças no cenário administrativo da Casa e ao lapso temporal de seis anos desde a sua concepção. Em um ambiente no qual os riscos de segurança de informação mudam constantemente, esse lapso temporal pode indicar significativa desatualização das ações previstas, o que foi ratificado nas entrevistas realizadas[29].

57. Destarte, constata-se que persistem os riscos estruturantes relativos à eficácia das ações do CGSI enquanto não houver clareza sobre qual unidade (ou unidades) será responsável por implementar as suas competências operacionais, a nível corporativo.

[28] Disponível em: https://www2.camara.leg.br/legin/int/atomes/2012/atodamesa-47-16-julho-2012-773827-publicacaooriginal-137096-cd-mesa.html, art. 8º, § 3º, V-VIII. Acesso em: 2 dez. 2020.
[29] A técnica de entrevistas não permite, em tais casos, a generalização das percepções captadas. Contudo, dada a relevância das unidades envolvidas e a proficiência dos servidores consultados, além dos testes substantivos e análises realizadas, pode-se chegar, com um nível razoável de segurança, às conclusões apresentadas.

4.2.8. Recomendações

a) Recomendar ao Comitê de Gestão em Segurança da Informação (CGSI) que revise e atualize o Plano de Ação em Segurança da Informação (PASI), refletindo as atuais demandas institucionais.
Prazo: 180 dias.

b) Recomendar à Diretoria-Geral, na qualidade de unidade coordenadora do Comitê de Gestão Estratégica (CGE), que identifique a(s) unidade(s) organizacional(is) responsável(is) pela implementação das ações de segurança da informação em nível corporativo, com as respectivas competências, como é o caso das ações preconizadas pelo PASI.
Prazo: 180 dias.

4.3. Lacuna na realização de reuniões ordinárias realizadas pelo CGSI

4.3.1. Situação encontrada

58. Não conformidade da periodicidade de reuniões ordinárias realizadas pelo CGSI, conforme estipulado no Artigo 5º da Portaria n. 407, de 30/09/2013, da Diretoria-Geral, que prevê a realização de uma reunião ordinária por mês.

4.3.2. Critérios

a) Portaria de instalação e de funcionamento do CGSI, Artigo 5º (Portaria n. 407, de 30/09/2013).

4.3.3. Evidências

a) Atas das reuniões do CGSI.

4.3.4. Causa

a) Falta de adequação da norma instituidora do CGSI no tocante ao quantitativo mínimo ou periodicidade de reuniões ordinárias.

4.3.5. Efeitos potenciais

a) Ausência de padronização das reuniões;

b) Atrasos nas entregas;

c) Deficiência no acompanhamento das atividades.

4.3.6. Esclarecimento dos Auditados

59. A equipe de auditoria questionou a gestão sobre a necessidade de uma previsão normativa da periodicidade das reuniões do CGSI.

60. A Ditec informou que:

> Considerando-se apenas as reuniões de natureza deliberativa, com vistas à tomada de decisões estratégicas, entende-se que a frequência poderia ser diminuída. Nesse sentido, tal alteração já foi aprovada pelo CGSI por ocasião da 18a Reunião Ordinária, realizada em 08/08/2019. A proposta de alteração dos normativos do CGSI, incluindo a periodicidade das reuniões, foi encaminhada à área responsável pela governança dos Comitês no início de 2020, com vistas à condução do processo de aprovação.

61. Por sua vez, a DG destacou:

> A Assessoria de Projetos e Gestão (Aproge), em conjunto com os Comitês Temáticos, deu início a um trabalho de atualização dos normativos que instituíram cada uma dessas instâncias. No escopo da revisão do CGSI, está prevista a revisão do número de reuniões ordinárias, considerando que, na prática, o número atual não se mostrou adequado. Não obstante, a partir da última Reunião de Avaliação da Estratégia (RAE), na qual foi apresentado um panorama dos atuais Comitês Temáticos, identificou-se a necessidade de uma revisão mais profunda dessas instâncias, à luz das diretrizes da proposta de Reforma Administrativa da Casa. Nesse sentido, optou-se por adiar a apresentação das propostas de alterações naquele momento e deu-se início ao planejamento de uma ação que será implementada a partir da segunda quinzena de janeiro. Nesse trabalho conjunto a ser desenvolvido pela Aproge, membros dos Comitês e especialistas nos temas em questão, serão reavaliadas as diretrizes, competências, composição, natureza e a vocação de cada um deles.

62. Por fim, o Cedi destacou que cabe ao coordenador do CGSI responder essa questão.

4.3.7. Análise

63. Ao examinar o teor das reuniões do CGSI percebe-se a relevância para a Casa dos temas abordados. No âmbito desse Comitê, foram apreciados assuntos relevantes institucionalmente, quais sejam: definição de uma norma de classificação de informações, gestão de riscos de segurança da informação, campanha institucional de conscientização em segurança da informação, adoção de serviços de computação em nuvem e Lei Geral de Proteção de Dados (Lei 13.709, de 2018).

64. Conforme a Portaria DG n. 407, de 30/09/2013, que dispõe sobre a instalação do CGSI: “Art. 5º O CGSI reunir-se-á, ordinariamente, uma vez a cada mês”. Entretanto, a avaliação quantitativa das atas das reuniões do CGSI mostrou o resultado exibido pela Tabela 1.

Tabela 1- Quantitativo de atas das reuniões anuais do CGSI

Ano	Quantidade de atas reuniões anuais
2019	4
2018	3
2017	3

Fonte: Atas das reuniões do CGSI. Disponível em: https://camaranet.camara.leg.br/web/gestao-estrategica/atas. Acesso em 2 dez. 2020

65. Desta forma, fica claro que as reuniões do comitê não vêm sendo realizadas conforme preconizado pelo normativo, ao menos nos últimos quatro anos.

66. Sabe-se que há um acúmulo de atividades pelos membros do CGSI, já destacado anteriormente neste relatório. Todavia, observando-se sob o prisma

estrito da conformidade normativa, verifica-se que há necessidade do cumprimento do cronograma de reuniões, ou de se adaptar o regulamento a um calendário exequível e coerente com as demandas enfrentadas pelo Comitê.

4.3.8. Recomendações

a) Recomendar à Diretoria-Geral (DG) que avalie o disposto na Portaria n. 407, de 30/9/2013, no tocante às reuniões do CGSI.
Prazo: 90 dias.

b) Recomendar ao CGSI que observe o calendário de reuniões previsto em sua portaria de instalação e funcionamento.
Prazo: 90 dias.

5. Benefícios potenciais da ação de controle

67. Em observância ao Artigo 3º da Portaria n. 2, da Secretaria de Controle Interno, de 22 de fevereiro de 2013, registre-se que esta ação de controle visa aos seguintes benefícios potenciais:

a) melhoria no processo de gestão de riscos relativos à governança e a gestão do desenvolvimento e implementação de níveis e estratégias de proteção de dados, segurança e privacidade;
b) aumento da eficiência das ações deliberadas no âmbito do CGSI;
c) melhoria no acompanhamento das ações preconizadas no PASI;
d) melhoria do ambiente de conformidade do CGSI.

6. Conclusões

68. Esta auditoria teve por objetivo avaliar aspectos de governança e de gestão do processo de trabalho de desenvolver e implementar níveis e estratégias de proteção de dados, segurança e privacidade.

69. Esse objeto é resultado da fusão dos processos COBIT 5: APO 13 – Gerenciar Segurança e DSS 05 – Gerenciar Serviço de Segurança e apresenta impacto direto em várias atividades da gestão, tais como: gerenciar o catálogo de serviços, gerenciar níveis de serviço e construir solução de TIC.

70. No decorrer da execução da referida ação de controle, constatou-se a inexistência de métodos diferenciados de autenticação para os usuários que realizavam ações sensíveis. Assim, verificou-se a necessidade de aperfeiçoar os níveis de segurança da informação para os perfis de acesso com maiores privilégios nos acessos remotos. Deste modo, a equipe de auditoria questionou a gestão sobre a existência de planos para implementar a autenticação em dois ou mais fatores, como forma de garantir esse tipo de acesso à distância.

71. A Ditec informou que o robustecimento do mecanismo de autenticação utilizado durante o acesso externo aos sistemas e serviços digitais da Câmara dos Deputados estava previsto no objetivo digital (OD6) - Aumento da Confiança Digital, um dos pilares da proposta de Estratégia de Transformação Digital da Câmara dos Deputados. Ademais, a unidade forneceu, em 13/5/2021, um plano de ação especificando situação, datas de entrega e usuários do Programa Confiança Digital, distribuído em três projetos: Robustecimento da Autenticação, do controle de permissões e da auditoria de serviços digitais; Login Cidadão 3.0; e, Central de Monitoramento de Eventos de Segurança da Informação. Devido ao fato de que as principais entregas relativas à fragilidade encontrada pela equipe de auditoria terem sido implementadas, ou estarem em via de implementação, considerou-se que o risco detectado foi mitigado, sem prejuízo de ser revisitado em futuras ações de controle.

72. Ao final dos trabalhos da auditoria, foram identificados riscos residuais ao testar outros controles, resultando em três pontos de auditoria devidamente suportados por suas respectivas evidências.

73. Por fim, registre-se o agradecimento aos servidores da DG, Aproge, Cedi, CGSI e Ditec que colaboraram com esta ação de controle, cujo valioso auxílio foi crucial para o desenvolvimento deste trabalho.

Brasília - DF, 25 de maio de 2021.