Instituto Brasileiro de Geografia e Estatística

Auditoria Interna (AUD)

RELATÓRIO DE AVALIAÇÃO

Gestão da Segurança da Informação e Comunicações, com ênfase em Cibersegurança

05 de dezembro de 2023

Ministério do Planejamento e Orçamento (MPO)
Fundação Instituto Brasileiro de Geografia e Estatística (IBGE)
Auditoria Interna (AUD)

RELATÓRIO DE AVALIAÇÃO

Objeto:	**Gestão da Segurança de Informação e Comunicações, com ênfase em Cibersegurança**
Unidade Gestora:	**Diretoria de Tecnologia da Informação (DTI) – Marcos Vinícius Ferreira Mazoni e Centro de Documentação e Disseminação de Informações (CDDI) – José Daniel Castro da Silva**

Relatório de Avaliação: 02/2023

Missão

Aumentar e proteger o valor organizacional do IBGE, fornecendo avaliação, assessoria e conhecimentos objetivos e baseados em riscos.

Avaliação

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA AUD?

Este relatório de auditoria tem como objetivo avaliar a Gestão da Segurança da Informação e Comunicações, com foco em Cibersegurança, e identificar eventuais vulnerabilidades e riscos associados. A auditoria se concentrou na avaliação das políticas, procedimentos, sistemas e práticas de segurança da organização, com o objetivo de garantir a confidencialidade, integridade e disponibilidade dos dados críticos nas unidades gestoras do objeto de auditoria, que são a Diretoria de Tecnologia da Informação (DTI) e o Centro de Documentação e Disseminação de Informações (CDDI).

Os critérios gerais para a avaliação da governança, dos processos que compõem a gestão de riscos e dos controles internos estão definidos na Política de Gestão de Riscos e na Metodologia de Gestão de Riscos do IBGE, em sua 3ª Edição, aprovada pela Resolução do Conselho Diretor (R.CD) nº 83, de 27/10/2022. A metodologia de trabalho de avaliação baseou-se no disposto na Instrução Normativa da Secretaria Federal de Controle da Controladoria-Geral da União (IN SFC/CGU) nº 3, de 09/06/2017, que aprovou o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (Manual de Orientações Técnicas – MOT).

POR QUE A AUD REALIZOU ESSE TRABALHO?

O processo de Gestão da Segurança da Informações e Comunicações, com ênfase em Cibersegurança, foi selecionada a partir da sugestão do Conselho Curador do IBGE.

A Cibersegurança é uma preocupação cada vez mais relevante em um mundo digital interconectado e sua implementação adequada é fundamental para a proteger dos dados pessoais, favorecendo a continuidade dos serviços TIC e preservando a reputação do IBGE.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUD? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Observou-se que esforços têm sido direcionados aos desafios da segurança da informação e comunicações da Instituição, sendo que foram identificados:

1. A não implementação do Plano de Gestão de Riscos do IBGE, com previsões específicas de reporte e comunicação ao CSI, e a inexistência de compartilhamento de informações com o CGOV;
2. O não mapeamento do processo "gerir segurança da informação e comunicações", dificultando melhor análise dos riscos e de eventual implementação de medidas de tratamento para a sua mitigação;
3. Ausência de um plano de capacitação contínua em segurança da informação e comunicações para servidores do IBGE que atuam diretamente com o assunto;
4. A não destinação de recursos orçamentários destacados da agenda TIC do IBGE, impossibilitando que o planejamento e a gestão das atividades de segurança da informação e comunicações ocorram com plena envergadura; e
5. Fragilidades na gestão de mídias sociais do IBGE, como a ausência de mapeamento dos processos; o estabelecimento de diretrizes claras para a sua gestão; a inexistência de autenticação multifator e a centralização de contas; e falta de plano de resposta a incidentes de segurança.

LISTA DE SIGLAS E ABREVIATURAS

AUD	Auditoria Interna do IBGE
CC	Conselho Curador
CD	Conselho Diretor
CDDI	Centro de Documentação e Disseminação de Informações
CGOV	Comitê de Governança, Riscos e Controles
CSI	Comitê de Segurança da Informação do IBGE
CTA	Coordenação de Treinamento e Aperfeiçoamento
DSIC/GSIPR	Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.
DPSI/SGD	Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital
DTI	Diretoria de Tecnologia da Informação
ENCE	Escola Nacional de Ciências Estatísticas/IBGE
ETIR	Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos
GPG	Gerência de Planejamento e Gestão
GT	Grupo de Trabalho
IBGE	Fundação Instituto Brasileiro de Geografia e Estatística
IN	Instrução Normativa
LGPD	Lei Geral de Proteção de Dados Pessoal
MPO	Ministério do Planejamento e Orçamento
MOT	Manual de Orientações Técnicas/CGU
RCD	Resolução do Conselho Diretor do IBGE
PAINT	Plano Anual de Auditoria Interna
PGP	Programa de Governança em Privacidade
POSIC	Política de Segurança da Informação e Comunicação
PPSI	Programa de Privacidade e Segurança da Informação
PSI	Política de Segurança da Informação
PP	Política de Privacidade de Dados
RIPD	Relatório de Impacto e Proteção de Dados Pessoais
SA	Solicitação de Auditoria
SAPC	Sistema de Administração de Pessoal Censitário

SEDGG/SGD	Secretaria de Gestão e Desempenho de Pessoal da Secretaria de Governo Digital
SDA	Sistema de Dados Administrativos do IBGE
SEI	Sistema Eletrônico de Informação
SGD	Secretaria de Governo Digital
SOC	*Security Operation Center*
SFC/CGU	Secretaria Federal de Controle da Controladoria-Geral da União

SUMÁRIO

INTRODUÇÃO 8

RESULTADOS DOS EXAMES 10

RECOMENDAÇÕES 16

CONCLUSÃO 19

EQUIPE DE AUDITORIA 22

ANEXO I 23

MANIFESTAÇÃO DA UNIDADE EXAMINADA E ANÁLISE DA EQUIPE DE AUDITORIA 23

INTRODUÇÃO

Este relatório de auditoria teve como objetivo avaliar a Gestão da Segurança da Informação e Comunicações, com ênfase em Cibersegurança, e identificar eventuais vulnerabilidades e riscos associados. A Auditoria Interna do IBGE concentrou-se em avaliar as políticas, procedimentos, sistemas e práticas de segurança da organização, com o intuito de garantir a confidencialidade, integridade e disponibilidade dos dados críticos. A Cibersegurança é uma agenda cada vez mais relevante em um mundo digital interconectado, e sua adequada implementação é essencial para proteger os ativos de informação e preservar a reputação e continuidade dos negócios da organização.

A Segurança da Informação é necessária para a proteção dos ativos de informação contra ameaças cibernéticas, como ataques de *hackers*, *malware*, roubo de dados e interrupções de serviços. Um incidente de segurança pode resultar em perdas financeiras significativas, danos à reputação da organização e violação da confiança da população e de parceiros institucionais. Portanto, é imperativo que o IBGE adote uma abordagem proativa e robusta em relação à cibersegurança, implementando controles adequados e promovendo a conscientização e a educação dos funcionários.

O processo de transformação digital, ao mesmo tempo em que disponibiliza aos cidadãos cada vez mais serviços digitalizados, acessíveis por meio de aplicativos e de sítios na Internet, torna as organizações públicas progressivamente mais dependentes de soluções de tecnologia da informação, em especial de ferramentas de software, bases de dados e sistemas informatizados.

As unidades gestoras do objeto de auditoria foram:

1. Diretoria de Tecnologia da Informação (DTI):
   A DTI é responsável por: planejar, desenvolver, implementar e manter os sistemas de informação e tecnologia; garantir o suporte tecnológico necessário para a realização das atividades de produção e disseminação de dados e informações estatísticas; e por desenvolver e gerenciar sistemas de coleta, processamento e análise de dados, além de garantir a segurança da informação e a integridade dos dados. Desempenha um papel estratégico na transformação digital do instituto, buscando aprimorar constantemente as práticas de gestão da informação, segurança cibernética e governança de tecnologia; e

2. Centro de Documentação e Disseminação de Informações (CDDI):
   O CDDI desempenha um papel crucial na gestão e acesso às informações do IBGE, fornecendo suporte para pesquisadores, estudantes, profissionais e o público em geral que buscam dados confiáveis e atualizados sobre o país. Desempenha atividades como: preservar e conservar os documentos e dados estatísticos e geográficos do IBGE, garantindo sua integridade e acessibilidade ao longo do tempo; disponibilizar as informações coletadas e organizadas pelo IBGE para o público; e oferecer serviços de atendimento ao público, auxiliando na busca e obtenção de informações específicas.

Os critérios gerais para avaliação da governança, processos de gestão de riscos e controles internos residem na Política de Gestão de Riscos e na Metodologia de Gestão de Riscos do IBGE, em sua 3ª Edição, aprovada pela Resolução do Conselho Diretor (R.CD) nº 83, de 27/10/2022.

A metodologia de trabalho de avaliação baseou-se no disposto da Instrução Normativa da Secretaria Federal de Controle da Controladoria-Geral da União (IN SFC/CGU) nº 3, de 09/06/2017, que aprovou o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (Manual de Orientações Técnicas – MOT), que serve de guia para o planejamento dos trabalhos individuais de auditoria, com foco em riscos, de forma a agregar valor à Unidade Auditada, identificando oportunidades para aperfeiçoamento dos processos de governança, gerenciamento de riscos e de controle.

Seguindo o referencial técnico do MOT e adotando a Metodologia de Gestão de Riscos do IBGE, a Auditoria Interna avaliou os riscos e controles do tema e, por meio de Matriz de Planejamento, individualizou as questões de auditoria a serem percorridas em cada um dos exames, a saber:

1. Qual a capacidade de resposta institucionalizada na prevenção a roubo de dados?

2. Qual a capacidade de resposta institucionalizada na prevenção do acesso não autorizado a dados?

3. Qual a capacidade de resposta institucionalizada para a continuidade dos serviços de TIC?

Assim, no curso do trabalho, foram editadas diversas Solicitações de Auditoria (SA) às Unidades do IBGE responsáveis e com envolvimento em cada um dos processos e subprocessos examinados, com a coleta e a análise de dados, possibilitando a documentação de evidências para eventuais provas relacionadas a achados de auditoria, registradas em papéis de trabalho.

Os resultados dos exames realizados foram apresentados e discutidos com os respectivos gestores das Unidades Auditadas, como achados de auditoria relacionados a melhorias operacionais ou eventuais identificações de exposição a riscos, tendo as manifestações sido documentadas e registradas em papéis de trabalho.

As recomendações dispostas neste Relatório consistem em propostas de ações com a finalidade de aprimorar controles internos, aperfeiçoar os processos e implementar medidas de mitigação de eventuais riscos, objetivando agregar valor à gestão.

RESULTADOS DOS EXAMES

1) **Não implementação do Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações (TIC), de forma estruturada e periódica, como previsto na Política de Segurança da Informação e Comunicações (POSIC), em consonância com a Política de Gestão de Riscos do IBGE, fragiliza o gerenciamento de riscos na Instituição e a comunicação de suas avaliações à Alta Administração**

   A POSIC estabelece no item 2.8 Gestão de Riscos que o "*Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações deve ser desenvolvido e atualizado periodicamente para evitar que ameaças, de origem natural ou humana, de forma acidental ou proposital, explorem as vulnerabilidades dos ativos provocando perdas e prejuízos para a Instituição, através da destruição não autorizada, revelação ou exposição indevida, adulteração, dano, indisponibilidade ou perda de informações da organização.*".

   Segundo informações prestadas pelos gestores, esforços foram desenvolvidos em 2018 em uma iniciativa de gerenciamento dos riscos em TIC, mas a sua continuidade e a manutenção do documento atualizado mostrou-se bastante difícil frente a todos os outros esforços de TIC que foram priorizados neste período. Desde 2020, informou-se que a Diretoria de Tecnologia da Informação vem trabalhando na construção de um novo documento de gestão de riscos, seguindo a metodologia estabelecida no IBGE, mas esse trabalho é bastante extenso e árduo, requerendo a participação conjunta de várias áreas e a sua priorização acaba sendo diminuída frente às questões operacionais de TIC do IBGE.

   Considerando que a Política de Gestão de Riscos do IBGE prevê, em menção específica na página 13, que "*A gestão de riscos de segurança da informação segue as orientações da POSIC (Política de Segurança da Informação e Comunicações do IBGE) (IBGE, 2017b) e os documentos e normas aplicáveis, como a ABNT NBR ISO/IEC 27005 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2011).*", as diretrizes relacionadas ao assunto devem ser propostas pelo Comitê de Segurança da Informação e Comunicações do IBGE ao Conselho Diretor, que é a instância máxima de governança da Instituição.

   Neste sentido a não implementação estruturada e periódica do Plano de Gestão de Riscos em TIC fragiliza ainda mais o gerenciamento de riscos no IBGE, uma vez que não identifica e endereça todas as medidas de tratamento para eventos de riscos em TIC. Hoje o Plano de Gerenciamento de Riscos do IBGE conta com número bem restrito de projetos/processos listados com identificação, análise e tratamento de riscos, e a não implementação estruturada e periódica do gerenciamento dos riscos de TIC reforça a dificuldade da Instituição em elaborar e manter esse Plano.

   Adicionalmente, a inexistência de previsão normativa na POSIC para o reporte e a comunicação do Plano de Gestão de Riscos (estratégicos) em TIC e das respectivas avaliações do gerenciamento conduzidos pelo CSI ao Comitê de Governança, Riscos e Controles do IBGE (CGOV) não beneficia o acesso a informações relevantes para considerações em relação ao impacto em eventos de riscos nos processos da Cadeia de Valor do IBGE, não favorecendo uma visão consolidada e integrada da capacidade da organização de alcançar objetivos estratégicos e operacionais.

2) Ausência de mapeamento do processo de "gerir segurança da informação e comunicações", e de seus subprocessos, não permite se dispor de informações sobre o assunto, reduz a capacidade das equipes de debaterem aspectos para melhoria e não favorece uma avaliação dos riscos associados, identificando os eventuais impactos e as medidas de tratamento a serem executadas

Na avaliação referente ao contexto da governança e o gerenciamento de riscos, em relação à existência de processos modelados para o gerenciamento de vulnerabilidades para os dispositivos de redes, subprocesso de "gerir segurança da informação e comunicações" o gestor informou que ainda não há documentação formal do subprocesso, o que se deve à carência de pessoal. Entretanto, há esforços no sentido de documentar parte dos processos e de manter registros das vulnerabilidades, eventos e incidentes. (SA_2022.5.01.03).

Diante o exposto, por consequência, a área ainda não possui um processo formalizado para identificar, avaliar e tratar os riscos relacionados à segurança da informação.

Cabe ressaltar que a falta de documentação detalhada sobre como as informações que são coletadas, processadas, armazenadas e transmitidas torna os processos dependentes do conhecimento e compromisso dos profissionais que atuam na diretoria, comprometendo esse trabalho no futuro uma vez que dificulta a passagem de conhecimento para novas equipes.

3) Ausência de plano de capacitação contínua direcionada aos servidores que atuam diretamente em segurança da informação e comunicações na DTI

Por meio de indagações formuladas à DTI, foi constatado que não houve capacitação, nos últimos 3 anos, dentre os servidores que operam nas seguintes gerências (R.CD-IBGE nº 87/2022, de 04/11/2022):

1. *Gerência de Segurança da Informação e Comunicações* – DTI/GESEG, com 1 gerente, 1 tecnologista efetivo e 1 analista temporário;
2. *Gerência de Gestão de Incidentes* – DTI/GESEG/GINC, com 1 gerente e 1 tecnologista efetivo;
3. *Gerência de Proteção de Dados Institucionais* – DTI/COTEC/GINFR/GPDI, com 1 gerente e 1 analista efetivo; e
4. *Gerência de Segurança de Redes* – DTI/COTEL/GSER, com 1 gerente, 2 analistas efetivos e 2 analistas temporários.

A capacitação na área de segurança da informação e comunicações não apenas proporciona o conhecimento técnico para identificar e mitigar ameaças cibernéticas, mas também possibilitaria a promoção de uma cultura organizacional consciente da importância da segurança.

Nesse cenário, compreender continuamente e aplicar práticas eficazes de proteção de dados nunca foi tão crucial, tendo em vista que a crescente interconexão digital e a proliferação de dados sensíveis têm gerado uma necessidade urgente por capacitação em segurança da informação e comunicações.

Com a constante evolução das táticas de ataque cibernético, desde *phishing* até *ransomware* avançado, profissionais precisam estar atualizados sobre as mais recentes tendências e melhores práticas de segurança e respostas a incidentes.

Ao investir na capacitação em segurança da informação e comunicações, o IBGE poderá estar mais bem preparado para enfrentar os desafios cada vez mais sofisticados que o mundo digital apresenta, protegendo seus ativos e garantindo a confidencialidade, integridade e disponibilidade das informações.

4) Inexistência de dotação orçamentária própria fragiliza o planejamento e a gestão das atividades de segurança da informação e comunicações no IBGE

Por meio das informações obtidas durante a reunião realizada com a DTI/COTEL, ficou evidente a existência de dificuldades orçamentárias para ampliação e renovação de ativos de TIC, o que é notadamente causado pela ausência de um orçamento exclusivamente destinado a cobrir os gastos, investimentos e as atividades específicas ligados à segurança da informação e comunicações.

Essa situação cria um ambiente propício para a potencialização de riscos, uma vez que as questões orçamentárias internas podem resultar em uma distribuição de recursos que seja complicada para executar a renovação de licenças de softwares ou realizar atualizações na infraestrutura relacionadas diretamente a segurança da informação e comunicações.

Foi mencionado que essa situação já ocorreu em várias ocasiões anteriores, especialmente quando melhorias e investimentos na modernização da infraestrutura dependem de crédito vinculado às operações censitárias.

Para mitigar os riscos associados à segurança da informação e comunicações é necessária a dotação orçamentária própria, para evitar a competição por recursos com outras iniciativas e projetos TIC.

5) Ausência de normatização e formalização relacionada à gestão, ao controle e à segurança das mídias sociais do IBGE

Verificou-se, levando em consideração as informações contidas nas manifestações dos gestores em resposta às SA 2022.5.01.02, SA 2022.5.01.05 e SA 2022.5.01.06, que os subprocessos de gestão da segurança da informação e comunicações relacionados às mídias sociais não estão devidamente formalizados, inexistindo documentação que atribua responsáveis, objetivos na utilização das mídias sociais, fluxos de processo, gerenciamento de acesso de servidores às contas de mídias sociais. Tudo, portanto, é feito de forma ad hoc. Em que pese de forma abrangente - por englobar a segurança cibernética em sentido amplo, que não se limita às mídias sociais - ter sido criada, por meio da Resolução do Conselho Diretor do IBGE nº 120, de 12 de dezembro de 2022, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) no âmbito do IBGE, a norma não traz uma previsão da atuação sobre aspectos relacionados às mídias sociais.

Elaborar documentação que atribua responsáveis, defina objetivos, estabeleça fluxos de processo e regule o gerenciamento de acesso às contas de mídias sociais é crucial para garantir uma gestão estruturada e eficaz das plataformas online de uma organização. Isso promove a transparência na responsabilidade, alinha as ações com metas institucionais claras, otimiza a eficiência operacional, protege contra riscos de segurança e cibernéticos, permite uma resposta ágil a crises e assegura que a comunicação nas mídias sociais esteja alinhada com a visão e os valores da organização, contribuindo para o sucesso global da estratégia de mídias sociais.

6) [redacted]

[redacted]

[redacted]

7) [redacted]

[redacted]

[redacted]

8) Inexistência de plano de capacitação em segurança para servidores que atuam com mídias sociais

Nas respostas às SA 2022.5.01.02 e SA 2022.5.01.05, verifica-se que foi elaborado o curso EAD de Segurança da Informação e Comunicações, que faz parte do conjunto de cursos da Escola Virtual do IBGE. O curso é obrigatório para todos os funcionários no momento do lançamento e faz parte da trilha de cursos para novos servidores. Contudo, não foi verificado o incentivo para que servidores que atuam com as mídias sociais organizacionais realizem tal capacitação e outras relacionadas à segurança da informação e comunicações. A necessidade de capacitação é importante, pois foi relatado – pela equipe técnica da DTI em resposta às supracitadas solicitações de auditoria, que a ocorrência de hackeamentos foi ocasionada pela falta de boas práticas para o uso e gerenciamento das contas das mídias sociais.

Implementar um plano de capacitação em segurança para servidores que atuam com mídias sociais é essencial para fortalecer a postura de defesa da organização online. Esse treinamento não apenas sensibiliza os servidores para ameaças cibernéticas, mas também os capacita a identificar e mitigar riscos, proteger informações confidenciais, garantir a conformidade regulatória e manter a integridade das contas de mídias sociais, resultando em uma presença online mais segura e confiável, crucial para a reputação e segurança do IBGE.

RECOMENDAÇÕES

1. Desenvolver o Plano de Gestão de Riscos do IBGE, conforme previsto na POSIC, e avaliar o estabelecimento de previsão específica quanto ao reporte e à comunicação do gerenciamento conduzidos pelo Comitê de Segurança da Informação e Comunicações (CSI) ao CGOV, inclusive quanto às análises do gerenciamento conduzido pelo CSI, de forma a favorecer considerações em relação ao impacto em eventos de riscos nos processos da Cadeia de Valor do IBGE, permitindo uma visão consolidada e integrada da capacidade da organização de alcançar objetivos estratégicos e operacionais.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 1

2. Avaliar o mapeamento do processo “gerir segurança da informação e comunicações”, bem como seus subprocessos, de forma a favorecer a avaliação de riscos os quais os dispositivos de redes formalmente constituídos estão expostos, identificando os eventos, seus impactos, e as respectivas medidas de tratamento objetivando a capacidade de resposta do IBGE de atuar rapidamente quando da ocorrência de um incidente.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 2

3. Elaborar plano de capacitação contínua em segurança da informação contribuindo para o desenvolvimento dos servidores diretamente ligados ao tema, que também, em algum nível e detalhamento, possa ser destinado ao avanço do conhecimento e atualização profissional dos servidores das demais Unidades do IBGE, favorecendo a disseminação da cultura e a adoção das melhores práticas existentes.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 3

4. Avaliar a possibilidade de atribuir dotação orçamentária própria e em rubrica específica para o planejamento e a condução das atividades de gestão da segurança da informação e comunicações, segregada das demais previsões de investimento e custeio de tecnologia da informação do IBGE, com o objetivo de minimizar a competição da administração dos recursos com destinados à operação.

   Nível de criticidade: Alto

   Unidade Administrativa responsável: DTI

   Achado de Auditoria: 4

5. Avaliar o mapeamento do processo de gerir relacionamento por meio das mídias sociais, definindo objetivos, estruturando a modelagem das atividades, a característica das funções de trabalho e as atribuições dos gestores das mídias sociais do IBGE, possibilitando a indicação dos servidores responsáveis por cada mídia social, publicitando a orientação normativa e as divulgações que ocorrem em cada plataforma.

   Nível de Criticidade: Alto

   Unidade Administrativa responsável: CDDI

   Achados de Auditoria: 5 e 6

6. [redacted]

7. [redacted]

8. Instituir como atividade de trabalho dos servidores que atuam na gestão de mídias sociais a necessidade de capacitação continuada em segurança da informação e comunicações, adotando, por exemplo, a necessidade de performarem os cursos de educação à distância (EAD) do tema, disponibilizados pela DTI, além da participação em treinamentos e seminários sobre segurança das mídias sociais, favorecendo às medidas de segurança relacionada ao IBGE.

   Nível de Criticidade: Médio

   Unidade Administrativa responsável: CDDI

   Achados de Auditoria: 7 e 8

CONCLUSÃO

Apresentamos a seguir, as respostas às questões de auditoria propostas no planejamento da avaliação da Gestão da Segurança da Informação e Comunicações, com ênfase em Cibersegurança, com base no resultado dos exames (achados de auditoria) e nas causas raízes que foram possíveis de identificação.

1. Qual a capacidade de resposta institucionalizada na prevenção a roubo de dados?

   e

2. Qual a capacidade de resposta institucionalizada na prevenção do acesso não autorizado a dados?

   Em que pese o IBGE possuir em sua Política de Segurança da Informação e Comunicação (POSIC) a previsão do Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações (TIC), o mesmo não foi implementado como estabelecido, de forma estruturada e periódica em consonância com a Política de Gestão de Riscos do IBGE, situação que fragiliza o gerenciamento de riscos da Instituição em relação à avaliação da capacidade de respostas a incidentes, como a roubo e ao acesso não autorizado a dados.

   Adicionalmente, há um grupo de trabalho da Diretoria de Tecnologia da Informação (DTI), Unidade Administrativa denominado Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), que possui a responsabilidade de atuar em relação à segurança cibernética, em observância à Política de Segurança da Informação e Comunicação da Instituição.

   Em que pese a existência da POSIC e da ETIR, observamos que (i) a não implementação estruturada e periódica do Plano de Gestão de Riscos em TIC fragiliza o gerenciamento de tais riscos no IBGE, impossibilitando a avaliação, a análise e o endereçamento de medidas de tratamento para a prevenção a tais eventos de riscos.

   Observou-se também a inexistência de mapeamento do processo “gerir segurança da informação e comunicações” da Cadeia de Valor do IBGE, e de seus subprocessos, não permitindo uma disposição ordenada de informações sobre o tema, impactando a identificação, avaliação e tratamento dos riscos relacionados à segurança da informação.

   Foi constatado ainda que nos últimos 3 anos os servidores que atuam diretamente com segurança da informação do IBGE, em Unidades Organizacionais da Diretoria de Tecnologia da Informação (DTI), bem como servidores que atuam com as mídias sociais da Instituição, do Centro de Documentação e Disseminação de Informações (CDDI) não realizaram capacitações e atualizações técnicas relacionadas à segurança da informação.

   Importante relatar ainda que, quanto às mídias sociais do IBGE, considerando o acesso por parte de servidores, contratados temporários e estagiários, não é possível afirmar que os controles internos dão razoável segurança quanto ao acesso não autorizado, uma vez que

foi constatada fragilidade na concessão, revogação e ausência de normatização e formalização relacionada à sua gestão.

3. Qual a capacidade de resposta institucionalizada para a continuidade dos serviços de TIC?

   A inexistência de dotação orçamentária destinada ao planejamento e à gestão das atividades de segurança da informação e comunicações cria um ambiente propício para a potencialização de riscos, uma vez que a atual alocação dos recursos à toda agenda TIC pode resultar em dificuldades para a distribuição do volume necessário para, por exemplo, a renovação de licenças de softwares ou a realização de atualizações na infraestrutura diretamente relacionada à segurança da informação e comunicações, contribuindo para à gestão da continuidade dos serviços de TIC.

   Cabe também ressaltar que ficou evidente a inexistência de plano de ação para a contenção de danos e a recuperação de acesso em caso de indisponibilidade dos serviços das mídias sociais, que ainda estaria em fase de formalização, mas sem previsão de operacionalização.

Para estabelecer uma estrutura sólida de segurança da informação e comunicações, é importante que a governança esteja plenamente estabelecida, considerando que reflete o conjunto de processos, políticas, normas e estratégias que definem como a segurança da informação e comunicações será tratada no IBGE como um todo. Ela deve estabelecer os princípios, objetivos e diretrizes gerais que nortearão as ações e decisões relacionadas à segurança da informação e comunicações.

Uma vez que a governança esteja estabelecida, a gestão propriamente dita de segurança da informação e comunicações deve ser operacionalizada com base nas diretrizes e políticas definidas na governança. A gestão da segurança da informação e comunicações refere-se às atividades diárias que cabe ao IBGE realizar para proteger suas informações, em especial, os dados pessoais. Essas atividades incluem o desenvolvimento e implementação de controles de segurança, o monitoramento contínuo de ameaças e vulnerabilidades, além da resposta a incidentes de segurança, entre outros subprocessos.

Desta forma, os objetivos estratégicos de “fortalecer a governança de TIC” e “ampliar a governança de dados” garantirão um ambiente corporativo mais resiliente, por meio da construção de um ambiente confiável e protegido para as informações e os dados pessoais custodiados pelo IBGE.

Por fim, a Auditoria Interna entende que os principais benefícios esperados pela implementação das recomendações apresentadas neste relatório, pelos gestores responsáveis do processo avaliado, são:

- ✓ Melhor avaliação de eventuais lacunas relacionadas à privacidade de dados, de forma a conduzir um monitoramento mais assertivo das atividades essenciais do ambiente de segurança da informação e comunicações.

- ✓ Avanços na proteção dos dados pessoais, impedindo o acesso não autorizado a informações pessoais e o roubo de dados;

- ✓ Melhorais na prevenção de ataques maliciosos, em função da minimização dos riscos inerentes;

- ✓ Aumento dos esforços de continuidade dos serviços de TIC, objetivando sustentar o alcance dos objetivos estratégicos; e

- ✓ Fortalecimento da governança, do gerenciamento de riscos e dos controles internos de gerir segurança da informação e comunicações, com efeito em maior aderência ao atendimento de exigências de Órgão de Supervisão e de Órgãos Externos de Controle.

CARLOS ALBERTO VIANNA COSTA
Auditor-Chefe
Auditoria Interna – AUD
IBGE

EQUIPE DE AUDITORIA

Servidor	Cargo
Supervisão da auditoria realizada	
Adilson da Silva Marques	Assistente Técnico
Desenvolvimento das atividades	
Arthur Santos Lettré	Assessor Técnico Especializado
Ennio Amorim Serrano Junior	Tecnologista de Inf. Geog. e Est.

ANEXO I

Manifestação da Unidade Examinada e Análise da Equipe de Auditoria

Os achados de auditoria e as recomendações associadas foram discutidos com os gestores da DTI e do CDDI em uma busca conjunta de soluções, por meio de reuniões específicas nos dias 25/10 e 01/11/2023, por meio da plataforma Webex.

Na oportunidade, os referidos gestores das Unidades compreenderam as constatações apresentadas e as sugestões indicadas pela Auditoria Interna do IBGE visando a mitigação de riscos e oportunidades e melhorias operacionais.

Os gestores da DTI decidiram por manifestar-se a respeito do Relatório incluindo informações no corpo do documento, e a Auditoria Interna do IBGE, no que coube, por existirem evidências e concordância, incluiu parte dos comentários ao Relatório.

Os gestores do CDDI realizaram comentários por meio de e-mail, que foram considerados na versão final deste Relatório.

Foi informado que, de acordo com o previsto no Art. 4º da Norma de Tratamento dos Achados e Recomendações formulados pela Auditoria Interna do IBGE e de Solicitações, Recomendações e Determinações por Órgãos Externos de Controle, aprovada pela Resolução do Conselho Curador nº 01/2022, de 23/05/2022, a partir do encaminhamento pela AUD do Relatório de Auditoria para as Unidades Auditadas, os gestores destas Unidades Auditadas indicarão o tratamento a ser dado para os respectivos achados e recomendações, no prazo máximo de até 30 dias contados do recebimento do Relatório da Auditoria Interna.

Manifestações das Unidades:

DTI:

1. Não implementação do Plano de Gestão de Riscos em Tecnologia da Informação e Comunicações (TIC), de forma estruturada e periódica, como previsto na Política de Segurança da Informação e Comunicações (POSIC), em consonância com a Política de Gestão de Riscos do IBGE, fragiliza o gerenciamento de riscos na Instituição e a comunicação de suas avaliações à Alta Administração

Cabe ressaltar, que o Plano de Gestão de Riscos de TIC que está em elaboração é voltado aos riscos operacionais que não precisam ser necessariamente informados e apresentados ao CGOV, inclusive por conta da alta complexidade dos assuntos técnicos e pela questão da exposição de fragilidades que possam existir no ambiente.

CDDI:

5. Informalidade na condução das atividades expõe a riscos a gestão, o controle e a segurança da informação das mídias sociais do IBGE

O texto proposto no Resultados dos Exames está perfeito, bem como o que foi colocado no item Recomendações.

Cabe a médio prazo, a elaboração de um documento pela Coordenação de Marketing, para mapear e registrar os objetivos e fluxos de trabalho sobre as redes sociais, estabelecendo as áreas e o perfil dos responsáveis por essas atividades. Entendemos que esse documento deverá ser chancelado pela direção através de uma RCD. Não sabemos se cabe, nesse sentido, a inclusão da previsão da atuação sobre aspectos relacionados às mídias sociais junto à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), visto que atualmente não está contemplada nessa norma.

6. Necessidade de intensificar as medidas de segurança e o controle de acesso às mídias sociais da Instituição

O texto para esse tópico está bem completo. Acreditamos que os pontos críticos apontados devem ter suas soluções contemplada no documento de formalização das atividades do IBGE nas redes sociais. As medidas de segurança propostas nas Recomendações devem ser aplicadas tão logo possível, independente da validação de uma R.CD sobre gestão das redes sociais do IBGE.

7. Ausência de plano de ação para contenção de danos e a recuperação de acesso e conteúdo em caso de invasão às mídias sociais do IBGE

Sobre esse tópico, entendemos que a proteção e recuperação de acessos em caso de ataques às redes sociais oficiais é de responsabilidade de cada plataforma, não cabendo ao IBGE, especificamente aos gestores das mídias sociais e da área de segurança da informação essa atribuição. Contudo, as ações para recuperação de qualquer perfil devem estar relacionadas no documento. Achamos que nos casos de ataques, é válido ter um apoio da direção e/ou de outros órgãos públicos como intercessores e salvaguardas dos perfis oficiais do Governo Federal, junto às plataformas digitais, como a Meta e YouTube, por exemplo.

Nas Recomendações desse item, acho que deveria constar a relevância de se ter um suporte federal para casos de ataques à algum perfil do governo nas redes sociais. Talvez, a Secretaria de Comunicação do Governo Federal (SECOM) pudesse ser uma instância a ser acionada nessas situações.

8. Inexistência de plano de capacitação em segurança da informação e comunicações para os servidores que atuam com as mídias sociais

O texto apresentado é relevante e na nossa avaliação a capacitação continuada em segurança da informação e comunicações deve ser um pré-requisito para atuar como integrante da equipe das redes sociais, devendo constar essa informação no documento de formalização das atividades relacionadas às mídias sociais.

Documento assinado eletronicamente por CARLOS ALBERTO VIANNA COSTA, Auditor-Chefe, em 5 de Dezembro de 2023, às 16:49:56, horário de Brasília, com fundamento legal no § 3º do Art. 4º do Decreto Nº 10.543, de 13 de Novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://transparenciasda.ibge.gov.br/docs/validador.jsf informando o código verificador 47192861508765160 18 e o código CRC 8CD1BAC0.