AUDITORIA INTEGRADA

RELATÓRIO FINAL DE AUDITORIA

Processo nº 4.093/18-e

Avaliação dos recursos de TIC empregados no suporte ao aprendizado dos alunos da rede pública de ensino e dos mecanismos de segurança da informação dos sistemas de gestão escolar

Brasília 2018

Resumo Executivo

A presente auditoria integrada foi realizada na Secretaria de Estado de Educação do Distrito Federal – SEEDF, em cumprimento ao PGA 2018, tendo como objeto os principais recursos de tecnologia da informação e comunicação (TIC) disponibilizados pela SEEDF no suporte ao ensino educacional do DF, a segurança da informação dos sistemas de gestão escolar e a execução dos principais contratos de informática da SEEDF.

Cabe destacar que o uso da TIC pode contribuir no processo de ensino-aprendizagem, razão pela qual a SEEDF deve assegurar os recursos necessários de apoio educacional ao processo de informatização das escolas (link de dados, laboratórios, computadores, softwares educativos, suporte técnico e sistemas informatizados de apoio escolar).

Nesse sentido, foram realizadas visitas *in loco* às escolas públicas do DF, de forma a verificar o uso de recursos de TIC disponibilizados, bem como a infraestrutura instalada.

Além disso, a execução dos Contratos nºs 19/2013 (fornecimento de circuito de dados), 63/2011 e 23/2017 (Telefonia) e 06/2016 (suporte técnico) foi verificada bem como, no que concerne às práticas de segurança da informação adotadas pela SEEDF, o sistema i-Educar (software de gestão escolar) e o SIGEP (software de gestão de pessoas com a finalidade de auxiliar nas ações de gestão dos profissionais da educação nos âmbitos das unidades escolares e administrativas da SEEDF) foram avaliados.

O que o Tribunal buscou avaliar?

A fiscalização teve como objetivo geral verificar a regularidade da execução contratual dos principais fornecedores de TIC, os recursos de TIC empregados no suporte ao aprendizado do aluno e a integridade, confidencialidade e disponibilidade das informações dos sistemas de gestão escolar. Para alcançar esse objetivo, foram propostas 03 questões de auditoria:

1. Os contratos que envolvem TIC são executados em conformidade

com a legislação?

2. O uso dos recursos de TIC para fins educacionais foram suficientemente disponibilizados pela SEEDF às unidades escolares e são utilizados regularmente pelos alunos?

3. As informações geradas pelos sistemas de gestão escolar e de apoio são confidenciais, íntegras e disponíveis?

O que o Tribunal encontrou?

Os trabalhos desenvolvidos resultaram nos seguintes achados:

1 – Descontinuidade dos serviços de enlace de comunicação de dados nas unidades educacionais - Não houve o fiel cumprimento do contrato entre as partes, ocasionando o corte dos serviços pela contratada por falta de pagamento.

2 - Elevado índice de atendimento presencial, relativo à execução do Contrato nº 06/2016 – a ausência de monitoramento dos serviços prestados não permite identificar as razões do elevado número de ocorrências de escalonamento de atendimento para o nível presencial.

3 - Parque de computadores dos laboratórios de informática obsoleto - a falta de renovação do parque computacional instalado nos laboratórios de informática das escolas públicas do DF compromete a utilização do laboratório e o uso de novas tecnologias pelo aluno no processo ensino-aprendizagem.

4 - Baixa velocidade do link de acesso à Internet disponibilizado nos laboratórios de informática das unidades escolares públicas do DF – A velocidade média de acesso à Internet disponibilizada de 1 Mbps[1] nos laboratórios de informática não permite o uso dos computadores pelos alunos de forma eficiente.

5 - Baixo nível de maturidade na implementação de gestão de segurança da informação - a falta de gestão de segurança da informação compromete a confidencialidade, integridade e disponibilidade das informações.

6 - Capacidade insuficiente de a SEEDF atender às demandas do sistema i-Educar – o excesso de demandas acumuladas demonstra que a SEEDF possui

[1] Taxa de transferência (em megabit por segundo – Mbps) usualmente utilizada para medir a velocidade da Internet.

limitações para realizar a manutenção do sistema i-Educar.

Quais foram as proposições formuladas pela equipe de auditoria?

Entre as proposições formuladas, registram-se:

a) recomendar à Secretaria de Estado de Educação do DF – SEEDF que:

a.1) implemente ações no sentido de estabelecer procedimentos/roteiros com regras pré-determinadas para resolução imediata de incidentes pelo *Service Desk* (Central de Serviço), de forma a evitar o escalonamento de incidentes/demandas de usuários, em conformidade com o ITIL – gestão de incidentes e COBIT DS8;

a.2) estabeleça mecanismos de controle que permitam o monitoramento dos serviços prestados, nos termos do art. 20 da IN 04/2014-SLTI/MPOG;

a.3) adote as medidas necessárias visando atualizar o parque tecnológico dos laboratórios das escolas públicas do DF, de forma a fomentar o uso dos recursos tecnológicos para melhoria do fluxo escolar e da aprendizagem (meta/estratégia 7.12 do PNE), intensificando, por exemplo, o uso de recursos do Proinfo e celebração de acordos entre órgãos públicos para cessão de equipamentos;

a.4) reestabeleça o fluxo normal de atendimento das demandas represadas do sistema i-Educar, em conformidade com as melhores práticas de mercado (COBIT 5: BAI03.03, BAI03.03 e BAI09);

b) determinar à Secretaria de Estado de Educação do DF – SEEDF que:

b.1) implemente ações de contingência eficazes e, a médio prazo, realize processo licitatório com a finalidade de prover o acesso à Internet para utilização dos sistemas de apoio escolar,

considerando a ineficiência do PDAF como opção de contingência, nos termos do inciso VII da IN SLTI nº 04/2014;

b.2) elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27014:2013);

b.3) tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso aos sistemas críticos, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT ISO 27.001 e ABNT ISO 27.005;

b.4) passe a adotar abordagem baseada em riscos para segurança da informação conforme estabelece a ISO 27.001, ISO 27.005 e ISO 27.014;

b.5) elabore e faça uso de termo que cientifiquem os usuários dos sistemas de suas responsabilidades e obrigações e indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos assinados pelos usuários;

b.6) promova a melhoria contínua dos processos e produtos de segurança da informação, de acordo com as boas práticas (APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança do COBIT 5.0);

b.7) implante sistema automatizado de gestão de acessos e autorizações aos sistemas i-Educar e SIGEP, com validação periódica de cadastros por parte dos titulares das unidades administrativas de forma a padronizar a gestão administrativa de pessoal operando com a gestão de acesso de sistemas aos servidores da SEEDF.

Quais os benefícios esperados com a atuação do Tribunal?

Espera-se, com a adoção das medidas propostas pelo Tribunal, impulsionar a gestão de tecnologia da informação e comunicação da SEEDF, a fim de que as seguintes condições sejam satisfeitas:

a) garantir a disponibilidade de acesso à Internet para uso dos sistemas de apoio escolar pelas unidades escolares;

b) melhoria na prestação de serviço realizado pelo *Service Desk e* economia de recursos públicos;

c) utilização plena do laboratório de informática das unidades escolares com a ampliação da velocidade média de acesso à Internet e a renovação do parque de computadores;

d) estímulo ao aluno com o uso de novas tecnologias no processo ensino-aprendizagem;

e) diminuição do *backlog* atualmente existente do sistema i-Educar;

f) atendimento tempestivo das demandas do sistema i-Educar;

g) melhoria da gestão de segurança da informação, de recursos, de pessoas e de projetos educacionais pela SEEDF.

Sumário

1 Introdução 8
1.1 Apresentação 8
1.2 Identificação do Objeto 8
1.3 Contextualização 8
1.3.1 Fiscalizações Anteriores 10
1.4 Objetivos 10
1.4.1 Objetivo Geral 10
1.4.2 Objetivos Específicos 11
1.5 Escopo 11
1.6 Montante Fiscalizado 11
1.7 Metodologia 12
1.8 Critérios de auditoria 12
1.9 Avaliação de Controle Interno 13
2 Resultados da Auditoria 15
2.1 Questão 1 - Os contratos que envolvem TIC são executados em conformidade com a legislação e com as boas práticas de TI? 15
2.1.1 Achado 1 – Descontinuidade dos serviços de enlace de comunicação de dados nas unidades educacionais 15
2.1.2 Achado 2 – Elevado índice de atendimento presencial, relativo a execução do Contrato nº 06/2016 19
2.2 Questão 2 - O uso dos recursos de TIC para fins educacionais foram suficientemente disponibilizados pela SEEDF às unidades escolares e são utilizados regularmente pelos alunos? 25
2.2.1 Achado 3 – Parque de computadores dos laboratórios de informática obsoleto. 25
2.2.2 Achado 4 – baixa velocidade do link de acesso à Internet disponibilizado nos laboratórios de informática das unidades escolares públicas do DF 32
2.3 Questão 3 - As informações geradas pelos sistemas de gestão escolar e de apoio são confidenciais, íntegras e disponíveis? 37
2.3.1 Achado 5 – Baixo nível de maturidade de gestão de segurança da informação 37
2.3.2 Achado 6 – Capacidade insuficiente de a SEEDF atender às demandas do Sistema i-Educar 54
3 Conclusão 57
4 Proposições 58

1 Introdução

1.1 Apresentação

1. Trata-se de Auditoria Integrada realizada na Secretaria de Estado de Educação do Distrito Federal – SEEDF, em cumprimento ao PGA 2018.

2. A execução da presente auditoria compreendeu o período de 26 de abril a 25 junho de 2018.

1.2 Identificação do Objeto

3. A presente auditoria tem como objeto os principais recursos de tecnologia da informação e comunicação - TIC (ativos, serviços e sistemas de informação) disponibilizados pela SEEDF no suporte ao ensino educacional do DF, a segurança da informação dos sistemas de gestão escolar e de apoio educacional e a execução dos principais contratos de TIC da Secretaria de Estado de Educação do Distrito Federal – SEEDF.

1.3 Contextualização

4. A tecnologia da informação (TI) está se tornando um instrumento de intenso uso pela sociedade e pode contribuir como ferramenta de apoio às atividades de ensino.

5. A Lei de Diretrizes e Bases da Educação Nacional (LDB), Lei nº 9.394/96, estabeleceu como dever do Estado a progressiva extensão da obrigatoriedade do Ensino Médio. De acordo com a nova LDB, o Ensino Médio, sendo parte da educação escolar, “deverá vincular-se ao mundo do trabalho e à prática social” (Art.1º, §2º da Lei nº 9.394/96). Dessa forma, a perspectiva legal é de integrar duas dimensões diferenciadas, a do conhecimento e a da prática.

6. Nesse diapasão, o papel da TI na educação passa, necessariamente, da utilização básica de recursos tecnológicos (internet, planilhas eletrônicas, editores de textos...) por estudantes do ensino básico, fundamental e médio até a função da informática no auxílio à pesquisa e à produção de novos conhecimentos.

7. Segundo estudos[2], as condições de infraestrutura e de equipamentos de apoio didático são fatores importantes para a melhoria da aprendizagem, sendo, inclusive, objeto de diagnóstico periódico realizado pelo Censo Escolar, coordenado pelo Ministério da Educação – MEC.

8. Destaca-se que o uso da TI pode contribuir para incrementar a aprendizagem, notadamente, quando aliada à disponibilização de laboratório de informática para o estudante.

9. A tecnologia da informação integrada à proposta pedagógica está contemplada na estratégia 7.12, tecnologias educacionais[3], do Plano Nacional de Educação (PNE[4]). Essa estratégia preconiza o uso dos recursos tecnológicos para melhoria do fluxo escolar e da aprendizagem para a Educação Infantil, Ensino Fundamental e Médio.

10. No âmbito federal, foi criado o ProInfo - Programa Nacional de Informática na Educação, por meio da Portaria/MEC nº 522, de 09.04.97, com a finalidade de disseminar o uso pedagógico das tecnologias de informática e telecomunicações nas escolas públicas de ensino fundamental e médio, pertencentes às redes estadual e municipal.

11. O programa leva às escolas públicas computadores, recursos digitais e conteúdos educacionais. Em contrapartida, estados, Distrito Federal e municípios devem garantir a estrutura adequada para receber os laboratórios e capacitar os educadores para uso das máquinas e tecnologias.

12. Além disso, o FNDE – Fundo Nacional de Desenvolvimento da Educação, por meio do Programa Banda Larga nas Escolas (PBLE[5]), prevê o

---

[2] Arquivo associado ao processo (TI_na_Educacao_01.pdf e TI_na_Educacao02.pdf) ou DA_PT_19 e DA_PT_20.

[3] http://www.observatoriodopne.org.br/metas-pne/7-aprendizado-adequado-fluxo-adequado/estrategias/7-12-tecnologias-educacionais (Acesso em 12/09/2018)

[4] O PNE - Plano Nacional de Educação, Lei nº 13.005/2014, determina diretrizes, metas e estratégias para a política educacional dos próximos dez anos.

[5] PBLE - Programa Banda Larga nas Escolas (PBLE) foi lançado em 4 de abril de 2008 pelo governo federal, por meio do Decreto 6424, que altera o Plano Geral de Metas para a Universalização do Serviço Telefônico Fixo Comutado Prestado no Regime Público (PGMU). Fazem parte do programa as operadoras Telefônica, CTBC, Sercomtel e Oi/Brt.

atendimento/acesso à Internet para as escolas públicas urbanas, considerando as informações do censo da educação básica.

13. No caso em tela, a SEEDF deve assegurar os recursos necessários de apoio educacional ao processo de informatização das escolas (acesso à internet, equipamentos, softwares educativos, suporte técnico e sistemas informatizados de apoio escolar).

14. Cabe registrar o uso do sistema i-Educar[6] na gestão escolar do DF desde 2014, tornando necessário que a SEEDF assegure a confidencialidade, integridade e disponibilidade das informações geradas pelo sistema.

15. Desta forma, torna-se fundamental o aperfeiçoamento do uso das tecnologias da informação tanto no processo educacional por parte dos alunos quanto no processo de gestão por parte da SEEDF.

1.3.1 Fiscalizações Anteriores

16. Fiscalizações anteriores apontam para a necessidade de melhoria no processo de manutenção e desenvolvimento de softwares utilizados no apoio da gestão educacional, a exemplo de recomendações pretéritas desta Corte no âmbito dos processos nºs 1130/2014 (Gestão de profissionais de magistério), 8920/2015 (Programa de alimentação escolar), 14320/13 (Ações governamentais no Ensino Médio) e 8866/15 (Efetivação de Matrícula).

1.4 Objetivos

1.4.1 Objetivo Geral

17. Verificar a regularidade da execução contratual dos principais fornecedores de TIC, os recursos de TIC empregados no suporte ao aprendizado do aluno e a integridade, confidencialidade e disponibilidade das informações dos sistemas de gestão escolar.

---

[6] A principal finalidade do software é informatizar a gestão das informações educacionais, contribuindo com a racionalização do trabalho. No âmbito da SEEDF, o i-Educar foi formalizado por meio da Portaria nº 29, de 13 de fevereiro de 2014, a qual determinou a utilização plena do sistema para escrituração acadêmica em todas as unidades escolares.

1.4.2 Objetivos Específicos

18. Em função do objetivo geral da Auditoria, foram definidas as seguintes questões:

- Questão 1 - Os contratos que envolvem TIC são executados em conformidade com a legislação e com as boas práticas de TI?
- Questão 2 - O uso dos recursos de TIC para fins educacionais foram suficientemente disponibilizados pela SEEDF às unidades escolares e são utilizados regularmente pelos alunos?
- Questão 3 - As informações geradas pelos sistemas de gestão escolar e de apoio são confidenciais, íntegras e disponíveis?

1.5 Escopo

19. Foram analisados os seguintes contratos que envolvem TIC, com vigência no exercício de 2017, para verificação da regularidade da execução:

Tabela 1
Contratação de TIC pela SEEDF

Empresas	Serviços/Contratos	Valor Pago (R$)
OI S/A	Telefonia / Contratos nºs 63/2011 e 23/2017	1.086.344,94
OI S/A	Circuito de Dados MPLS / Contrato nº 19/2013	1.320.000,00
STEFANINI S/A	Desenvolvimento e Manutenção de TI / Contrato nº 06/2016	2.011.488,02

Fonte: SIGGO

20. Ainda, foram avaliados os sistemas de informação de apoio à gestão escolar da Secretaria de Estado de Educação do DF (i-Educar, SIGEP), no tocante à disponibilidade, integridade e confidencialidade das informações, bem como os recursos de TIC empregados na aprendizagem do aluno, a exemplo de computadores, internet, softwares, entre outros.

1.6 Montante Fiscalizado[7]

21. No último exercício (2017), considerando as maiores despesas com

[7] Tendo em conta a inexistência de Programa de Trabalho específico, não consta do montante examinado os gastos com gestão dos recursos de TIC empregados no suporte ao aprendizado, tampouco com a Segurança da Informação.

empresas prestadoras de serviços de tecnologia da informação, foi empenhado o montante de R$ 7.096.365,53 (sete milhões, noventa e seis mil, trezentos e sessenta e cinco reais e cinquenta e três centavos), conforme demonstrativo abaixo:

Tabela 2
Análise da Extensão dos Testes de Auditoria

CNPJ	Empresa	Valor Empenhado (R$)
4759978000192	AZ TECNOLOGIA LTDA	**82.375,00**
76535764032690	OI S/A	**1.405.000,76**
76535764000143	OI S/A	**1.705.831,00**
5423963000111	OI S/A	**513.334,00**
21262834000145	IDTCORP COMERCIO E TECNOLOGIA DA INFORMAÇÃO EIRELI	**69.500,00**
21748841000151	TECNETWORKING SERVIÇOS E SOLUÇÕES EM TI LTDA -ME	**55.354,20**
58069360000120	STEFANINI S/A	**3.264.970,57**
TOTAL		**7.096.365,53**

Fonte: SIGGO

1.7 Metodologia

22. Os procedimentos e técnicas utilizadas na execução da presente auditoria encontram-se registrados na Matriz de Planejamento.

23. Com a finalidade de verificar o uso dos recursos de TIC disponibilizados às escolas do DF para fins pedagógicos, definiu-se como população-alvo as escolas públicas de ensino infantil, fundamental e médio ligadas à SEEDF, localizadas em áreas urbanas/rurais do DF, excluídas as escolas técnicas por possuírem características singulares. Assim, selecionou-se aleatoriamente as escolas a serem visitadas dentro da população-alvo, levando-se em conta as escolas que possuem laboratórios de informática (Censo 2017) e a Diretoria Regional de Ensino – DRE/SEDF à qual se encontra vinculada, com a finalidade de assegurar que a amostra selecionada fosse representativa. Nesse sentido, visitou-se 31 escolas[8], representando 5% de cada Regional de Ensino do DF.

1.8 Critérios de auditoria

24. Os critérios de regularidade utilizados na presente auditoria foram extraídos da Instrução Normativa nº 04/2014-SLTI/MPOG, principal normativo que

[8] DA_PT_22 - Escolas visitadas e DA_26 - Parque dos computadores das escolas visitadas.

rege a contratação de bens e serviços públicos de tecnologia da informação, recepcionada no Distrito Federal pelo Decreto nº 34.667/2016, bem como da Lei nº 8.666/93 (artigos 66 ao 76).

25. As melhores práticas foram extraídas dos modelos COBIT 5[9] e NBR ISO/IEC 27002:13[10].

1.9 Avaliação de Controle Interno

26. Para o estabelecimento do Risco Inerente levou-se em consideração a materialidade dos valores envolvidos na Fiscalização (§ 19).

27. Considerando esse critério e de acordo com o Manual de Auditoria do TCDF, o Risco Inerente do objeto da Fiscalização pode ser considerado “Baixo”.

28. O Risco de Controle ficou situado, no nível “Fraco”, em razão da avaliação dos controles internos relacionados ao objeto da auditoria, considerando o questionário de governança/gestão respondido pela jurisdicionada (Processo TCDF nº 10.161/17), no qual a jurisdicionada, conforme gráfico abaixo, alcançou indicadores abaixo da média das demais instituições pesquisadas no GDF nas seguintes dimensões:

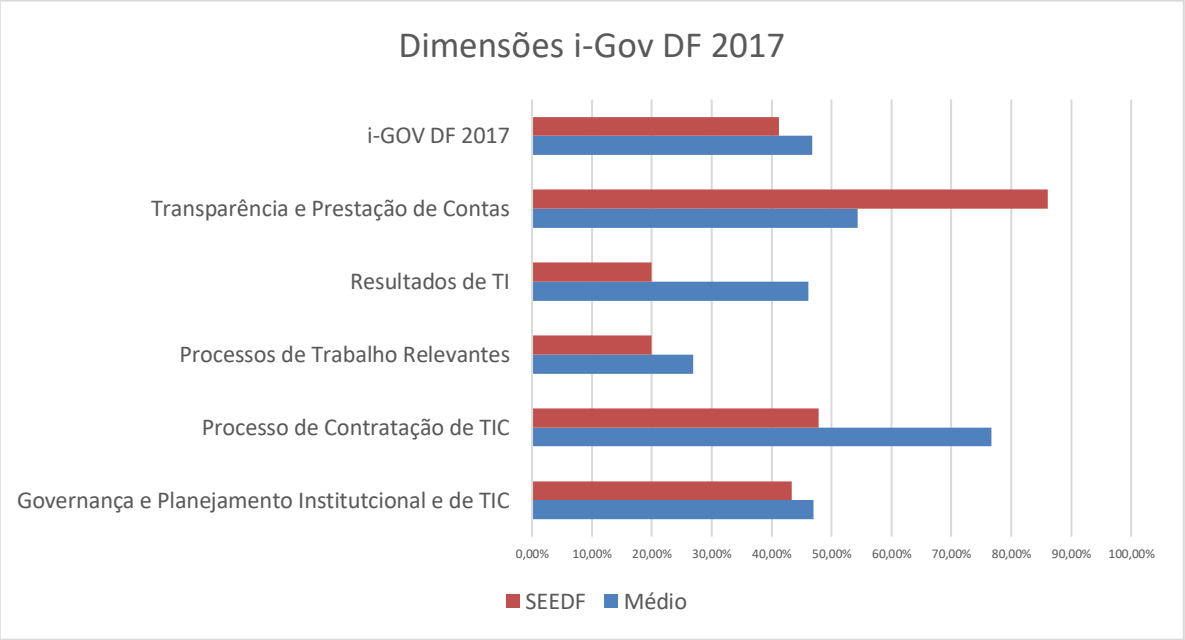
a. Resultados de TI para a sociedade;
b. Processos de Trabalho relevantes da unidade de TIC;
c. Processo de Contratação de TIC;
d. Governança e Planejamento Institucional e de TIC.

[9] COBIT é um modelo de governança e gestão de TI mantido pelo ISACA com a finalidade de apoiar os gestores e os profissionais no controle e gerenciamento dos processos de TI de forma lógica e estruturada, tendo como foco o relacionamento entre os objetivos de negócio com os objetivos de TI.

[10] Padrão para sistema de gestão da segurança da informação (ISMS - Information Security Management System), elaborada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI).

Gráfico 1

Governança de TIC GDF – 2017



Fonte: Relatório de Auditoria de Governança – Processo nº 10.161/17.

2 Resultados da Auditoria

2.1 Questão 1 - Os contratos que envolvem TIC são executados em conformidade com a legislação e com as boas práticas de TI?

No trabalho realizado, verificou-se a regular execução dos Contratos nºs 63/2011 e 23/2017 (Telefonia) e do Contrato nº 06/2016 (infraestrutura de TI), ao passo que no Contrato nº 19/2013 (enlace de comunicação de dados) houve a interrupção, pela empresa contratada, do fornecimento dos serviços no exercício de 2017, em razão da falta de pagamentos de débitos pretéritos. Em relação ao Contrato nº 06/2016 (infraestrutura de TI), observou-se elevado índice de atendimento presencial em comparação ao remoto.

2.1.1 Achado 1 – Descontinuidade dos serviços de enlace de comunicação de dados nas unidades educacionais

Critérios

29. O art. 66 da Lei 8.666/93 dispõe que o contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas desta Lei, respondendo cada uma pelas consequências de sua inexecução total ou parcial.

Análises e Evidências

30. O Contrato nº 19/2013[11], firmado entre a SEEDF e a empresa OI S/A em 01/03/2013, teve como objeto o fornecimento e implantação de solução global de comunicação de dados IP/MPLS em rede privada para as unidades administrativas e instituições de ensino da SEEDF, com valor anual contratado de R$ 5.798.689,92, nos termos do Processo nº 080.006.918/2012.

31. Segundo informações do executor do contrato, encaminhadas por meio de despacho à Coordenação de Informática da SEEDF[12], a partir de 16/05/2017, a empresa suspendeu gradativamente o fornecimento dos serviços, culminando com o desligamento total dos circuitos de dados em 27/07/2017, em virtude da falta de

[11] Arquivo associado ao processo (Contrato 19/2013 - Link de Dados.pdf) ou DA_28.

[12] Arquivo associado ao processo (Documento do Executor do contrato 19/2013.pdf) ou DA_PT_29.

pagamento de débitos oriundos de reconhecimento de dívidas. Em 01/03/2018, o Contrato extinguiu-se por decurso de prazo, segundo informação da área de contratos da SEEDF.

32. Em razão disso, os serviços administrativos realizados pelas unidades escolares sofreram forte impacto, vez que os sistemas de apoio da SEEDF (SEI, i-Educar e SIGEP) são acessados atualmente por meio da internet, ou seja, necessitam da utilização de serviços de comunicação de dados.

33. Diante desse cenário, a SEEDF autorizou as unidades escolares a contratarem serviços de comunicação de dados, por meio de verbas distribuídas pelo Programa de Descentralização Administrativa e Financeira – PDAF, nos termos da Circular Conjunta SUMTEC/SUPLAV/SUAG nº 1, de 13/06/17[13], considerando o desligamento dos serviços anteriormente fornecidos pela contratada, conforme se verifica no rack de parede com porta de vidro desativado. (vide foto).

Foto 1 - Laboratório do Centro de Ensino Médio 02 - Gama

Fonte: Visita da equipe *in loco*.

34. No entanto, restou evidenciado que a medida contingencialmente adotada pela SEEDF não surtiu efeito, vez que das 31 escolas visitadas apenas duas

[13] DA_30 – Resposta a Nota de Auditoria nº 02 – 4093/2018 – resposta à questão 7.

noticiaram que utilizavam a verba do PDAF[14].

35. Neste caso, constatou-se que a maioria[15] dos diretores entrevistados enfrentam dificuldades burocráticas para contratarem serviços de acesso à Internet por meio do PDAF, tais como: obtenção de certidão negativa, falta de interesse de as empresas proverem o serviço, atraso no recebimento da verba, entre outros.

36. Para resolver a falta de acesso à Internet para operar os sistemas administrativos da SEEDF, observou-se que a maioria[16] das escolas visitadas utilizam como forma de custeio desse serviço as Associações de Pais e Mestres - APM's e/ou cotização entre os servidores.

37. Por meio de resposta à Nota de Auditoria nº 02-4093/201817[18], a SEEDF noticiou que: *"A Subsecretaria de Modernização e Tecnologia, em cooperação com a SUTIC/SEPLAG, tem envidado esforços para ampliar o acesso à rede GDFNet, conforme Portaria Conjunta SEEDF/SEPLAG nº 15, de 21/9/17, publicada no DODF nº 183, de 22/9/17. Informamos também, que a SEEDF está trabalhando um novo processo licitatório para melhorar o serviço de internet nas Escolas (Administrativo e Pedagógico), com a previsão de publicação no primeiro semestre 2018".*

38. A situação atual demonstra a necessidade de a jurisdicionada retomar o fornecimento dos serviços de comunicação de dados e implantar solução global que atenda às unidades escolares, nos termos da IN SLTI/MPOG nº 04/2014, art.1319, inciso V, de forma a evitar as medidas contingenciais acima retratadas.

Causas

39. Planejamento deficiente na alocação dos recursos financeiros que ensejou a suspensão dos serviços pela contratada por falta de pagamento.

---

[14] Escola Classe Núcleo Rural Córrego do Atoleiro e Escola Classe Alta-Mir, localizadas em Planaltina.

[15] DA_PT_22 – Escolas Visitadas.

[16] DA_PT_22 – Escolas Visitadas.

[17] edoc nº E5C7FCE3 ou DA_30 - Resposta a Nota de Auditoria 02 - 4093/2018.

[18] NotaAud03_08_P4093_18RespostaSUMTEC.pdf (arquivo associado ao processo)

[19] *Art. 13. A Análise de Riscos será elaborada pela Equipe de Planejamento da Contratação contendo os seguintes itens: [...] V - definição das ações de contingência a serem tomadas caso os eventos correspondentes aos riscos se concretizem; e*

Efeitos

40. Utilização precária dos sistemas de apoio escolar pelas unidades escolares.

Considerações do Auditado

41. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, noticiou que (peça 19, fls. 1/2):

> *"... A Subsecretaria de Modernização e Tecnologia (SUMTEC) está ciente do impacto causado pela ausência de conexão à internet e das dificuldades encontradas pelos gestores na utilização de programas de recursos distritais e federais para contratação desse serviço. Nesta data, encontra-se em execução um projeto de integração da SEDF à GDFNet rede corporativa do Governo do DF, administrada pela Secretaria de Fazenda, Planejamento, Orçamento e Gestão (SEFP). A GDFNet já atende a outros órgãos do GDF e possui malha de distribuição inserida por todas as Regiões Administrativas. Assim, em parceria com a SEFP, foi elaborado cronograma para ligação das unidades escolares atendidas pela malha urbana. A SEEDF é, ainda, partícipe de processo licitatório, sob responsabilidade da SEFP para contratação de conexão de dados MPLS, a fim de retomar o fornecimento dos serviços àquelas unidades que, porventura, não puderem ser atendidas pela rede corporativa.*
>
> *Da mesma forma, encontra-se em fase de estudo de viabilidade técnica o processo para contratação de links destinados as unidades escolares do campo. "*

Posicionamento da equipe de auditoria

42. Verifica-se que a questão apresentada ainda carece de ações efetivas para suprir a demanda de acesso à Internet pelas unidades escolares da rede pública do DF, considerando o projeto de integração da SEEDF com a rede corporativa do GDF (GDFnet).

43. Em relação ao procedimento licitatório que trata da contratação de conexão de dados MPLS, que irá suprir a carência[20] de acesso à Internet das unidades escolares não atendidas pela rede GDFnet, verificou-se que se encontra na fase de elaboração do Estudo Técnico Preliminar – Processo SEI 00410-00023140/2017-90, conforme contato realizado com a Secretaria de Fazenda, Orçamento e Gestão – SEFP/DF

44. Cabe esclarecer que deixaremos de propor que a SEEDF adote medidas para concluir o processo de contratação com a finalidade de prover o regular acesso à internet para as unidades escolares da rede pública, uma vez que o aludido processo será conduzido pela SEFP de forma centralizada com as demandas de todos os órgãos do GDF, inclusive da SEEDF que será partícipe do certame.

Proposições

45. Sugere-se ao egrégio Plenário a proposição de determinar à SEEDF que:

a. implemente ações de contingência eficazes para suprir a carência de acesso à internet pelas unidades escolares, considerando a ineficácia do PDAF como opção de contingência, nos termos do artigo 13, inciso V, a IN SLTI MPOG nº 04/2014;

Benefícios Esperados

46. Garantir a disponibilidade de acesso à Internet para uso dos sistemas de apoio escolar.

2.1.2 Achado 2 – Elevado índice de atendimento presencial, relativo a execução do Contrato nº 06/2016

Critérios

47. A Instrução Normativa SLTI/MPOG nº 04/14, em seu art. 20, define que o modelo de gestão do contrato deverá contemplar as condições para gestão e

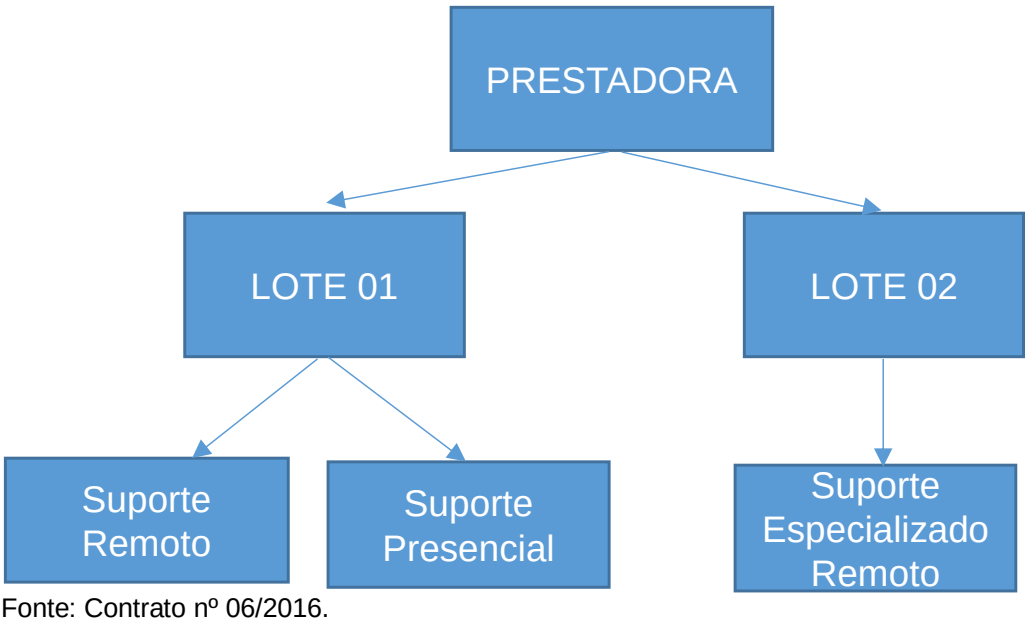
[20] SEI 00410-00023215/2017-32 – Demanda da SEEDF para acesso à Internet pelas unidades escolares da rede pública.

fiscalização do contrato, observando procedimentos de teste e inspeção, abrangendo metodologia, formas de avaliação da qualidade e adequação da Solução de Tecnologia da Informação às especificações funcionais e tecnológicas, observando a adoção de ferramentas, computacionais ou não, para implantação e acompanhamento dos indicadores estabelecidos. O COBIT, modelo de referência de gestão e governança de TIC, disciplina as atividades de gerenciamento de incidentes, por meio do domínio Entregar e Suportar, Processo DS8 - Gerenciar a Central de Serviço, bem como as práticas ITIL, referente à gestão de incidentes.

Análises e Evidências

48. O Contrato nº 06/2016, firmado entre a SEEDF e a empresa STEFANINI Consultoria e Assessoria em Informática S/A em 05/04/2016 (Processo n.º 098.002.735/2015), tem como objeto a prestação de serviços técnicos especializados em suporte técnico remoto e presencial, para sustentação de infraestrutura de TI e Auditoria de serviços em TI, com valor anual contratado de R$ 4.293.927,51, distribuídos da seguinte forma:

Fluxograma 1
Fluxo da prestação dos serviços, objeto do Contrato nº 06/2016



Fonte: Contrato nº 06/2016.

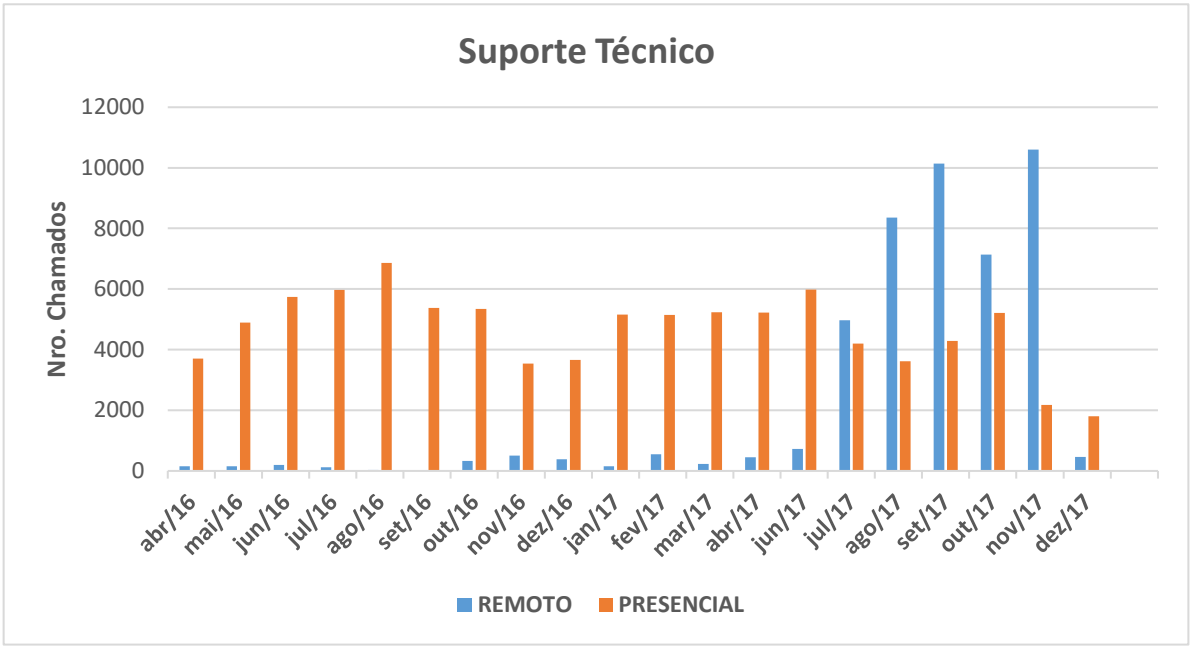
49. Os serviços prestados encontram-se categorizados por atividades[21] e níveis para atendimento aos servidores das sedes/regionais de ensino da SEEDF e

[21] Demanda de usuário, preventiva, evolutiva, corretiva, periódica e resolução de incidente.

das unidades escolares, conforme recomendado pelas boas práticas de mercado (ITIL[22]/COBIT).

50. Ao examinar os relatórios de atividades, relativo ao período de abril/2016 a dezembro/2017[23], verificou-se uma forte frequência de atendimento presencial executado pela contratada em comparação ao atendimento remoto (respectivamente, 93.102 chamados X 45.588 chamados), impactando na eficiência e nos custos do contrato, vejamos:

Gráfico 2



Fonte: Relatório de Atividades, relativo ao período de abr/2016 a dez/2017

51. Da mesma forma, observa-se elevado atendimento de chamados presenciais, relativo ao período de janeiro de 2018[24], mantendo a tendência evidenciada nos dois primeiros anos de execução contratual, o que demonstra a falta de monitoramento dos serviços prestados, nos termos do o art. 20 da IN 04/2014-SLTI/MPOG, vejamos:

[22] *ITIL - Technology Infrastructure Library, (ITIL)* é um conjunto de boas práticas para serem aplicadas na infraestrutura, operação e gerenciamento de serviços de tecnologia da informação.

[23] Arquivos associados ao processo (Chamados abril e dezembro/2016.rar e RelatoriosdeAtividadesStefannini jan-2017 a dez-2017.rar).

[24] Arquivo associado ao processo (SEEDF_Relatorio_Gerencial_de_Servicos_Janeiro_2018.pdf)

Gráfico 3

Fonte: Listagem de chamados, referente a janeiro/2018[25]

52. A situação acima evidenciada decorre de várias atividades/serviços escaladas para o nível de suporte presencial sem a devida necessidade[26], vez que podem ser executadas pela contratada, por meio de software de acesso remoto, a exemplo da conexão de área de trabalho remota do Windows, na qual um computador pode se conectar a outro que esteja conectado à mesma rede ou à internet.

53. O gerenciamento dos serviços contratados deve adotar práticas que priorizam o atendimento remoto, tais como: roteiros de atendimentos e regras pré-estabelecidas, de modo a resolver a demanda o mais tempestivamente possível, conforme preconizam os frameworks de mercado (ITIL – gestão de incidentes e COBIT DS8).

54. Neste caso, evidencia-se, ainda, o uso de recursos mais onerosos para a SEEDF na resolução dos incidentes/demandas dos usuários, vez que um atendimento remoto equivale a 0,4 UST (R$ 17,42 reais), ao passo que o suporte presencial custa o equivalente a 0,6 UST (R$ 26,14), conforme tabela abaixo:

[25] Arquivo associado ao processo (Listagem de Chamados JANEIRO2018.rar)

[26] Instalação/atualização de softwares e configuração de impressoras.

Tabela 3
Tipo de Atividade por Complexidade

Serviço	Escopo Resumido	Perfil Profissional	Complexidade
Central de Suporte (Service Desk)	Suporte Técnico Remoto	Técnico de Suporte Remoto	0,4
	Supervisão do Suporte Remoto	Supervisor de Suporte Remoto	0,5
	Suporte Técnico Presencial	Técnico de Suporte Presencial	0,6
	Supervisão do Suporte Presencial	Supervisor de Suporte Presencial	0,7
	Suporte Especializado em Sustentação de Rede	Administrador de Rede	1,2
Suporte Técnico Remoto e Presencial; Suporte Especializado em Sustentação de Rede, Segurança da Informação, Sustentação de Servidores, Administração de Dados e Administração de Banco de Dados e Auditoria	Suporte Especializado em Segurança da Informação	Analista de Segurança da Informação	1,3
	Suporte Especializado em Sustentação de Servidores e Operação	Analista de Rede	1,1

Fonte: Relatório gerencial de serviços, referente a janeiro/2018.

Causas

55. Inexistência de mecanismos de controle que permitam o monitoramento dos serviços prestados, em desacordo com o art. 20 da IN 04/2014-SLTI/MPOG e de regras pré-estabelecidas para resolução imediata de incidentes, conforme preconizam as boas práticas de mercado (COBIT DS8 e ITIL – gerenciamento de incidentes). Falhas na elaboração do termo de referência e especificação das obrigações contratuais.

Efeitos

56. Deficiência na prestação do serviço realizado. Escalonamento do incidente, ocasionando dilatação do prazo (intempestividade) e custo da resolução do incidente.

Considerações do Auditado

57. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, assim se manifestou (peça 19, fl. 2):

> *"... Informo que a contratação de empresa para prestação de serviços técnicos especializados de Solução de Tecnologia de Informação e Comunicação seguiu o disposto na Instrução Normativa MP/SLTI nº 04/2014 e que está aprimorando processos de prospecção de informação acerca de melhores práticas para contratação em TI adotadas no GDF, conforme informação repassada pela Diretoria de*

Infraestrutura e Operações.

Informo ainda que a equipe gestora do referido contrato revisou o documento e está repassando os atendimentos possíveis in loco para atendimento remoto. Estão em andamento as negociações para a renovação do contrato, em 05/04/2019, e os executores estão cientes da necessidade de incluir a determinação de prioridade de atendimentos remotos no documento a ser assinado pelas partes.

No que se refere ao monitoramento dos serviços prestados, a área técnica utiliza as ferramentas de controle Saiku Analytics, Zoho BI e Módulo Operador do Sistema de Service Desk - OTRS. "

Posicionamento da equipe de auditoria

58. As ações tomadas pela jurisdicionada são pertinentes e necessárias para o aprimoramento da gestão e uso corporativo dos recursos de TIC que se somam às medidas determinadas neste trabalho para o saneamento do presente Achado.

59. Desse modo, mantém-se inalterado o posicionamento da Equipe de Auditoria apresentado na versão prévia do Relatório de Auditoria.

Proposições

60. Sugere-se ao egrégio Plenário a proposição de recomendar à SEEDF que:

a. implemente ações no sentido de estabelecer procedimentos/roteiros com regras pré-determinadas para resolução imediata de incidentes pelo Service Desk (Central de Serviços), de forma a reduzir as ocorrências de escalonamento de incidentes/demandas de usuários, em conformidade com o ITIL – gestão de incidentes e COBIT DS8, bem como mecanismos de controle que permitam o monitoramento dos serviços prestados, nos termos do art. 20 da IN 04/2014-SLTI/MPOG.

Benefícios Esperados

61. Melhoria na prestação de serviço realizado pelo *Service Desk*, bem

assim a economia de recursos públicos.

2.2 Questão 2 - O uso dos recursos de TIC para fins educacionais foram suficientemente disponibilizados pela SEEDF às unidades escolares e são utilizados regularmente pelos alunos?

A maioria das escolas visitadas (80%) possui laboratórios de informática com instalações físicas satisfatórias, à exceção de 6 (seis) escolas que necessitam de melhorias pontuais nas instalações de cabeamento de rede[27]. No entanto, verificou-se dificuldades na utilização dos equipamentos/recursos de TIC dos laboratórios nas escolas em razão da obsolescência do parque computacional (41,7% dos computadores estão em manutenção e 79,1% apresentam mais de dez anos de uso)[28]. Quanto à disponibilidade de acesso à Internet aos alunos, constatou-se que todas as escolas possuem link de dados de 1 e 2 Mbps no laboratório de informática (custeado pelo FNDE), que compromete a utilização pelos alunos devido à baixa velocidade. Verificou-se que o software Linux educacional (Livre) encontra-se instalado nos computadores, beneficiando principalmente os alunos das séries iniciais (1ª a 4ª série), vez que o uso do software educativo requer pouca memória do computador e não precisa de acesso à internet. Nas demais séries (5ª a 8ª séries e ensino médio) verificou-se que os alunos utilizam o laboratório de informática basicamente para pesquisa na internet, segundo informações dos diretores de escola.

2.2.1 Achado 3 – Parque de computadores dos laboratórios de informática obsoleto.

Critérios

62. A meta/estratégia 7.12 – Tecnologias educacionais do Programa Nacional de Educação – PNE tem o objetivo de incentivar o desenvolvimento, selecionar, certificar e divulgar tecnologias educacionais para a educação infantil, o ensino fundamental e o ensino médio e incentivar práticas pedagógicas inovadoras que assegurem a melhoria do fluxo escolar e a aprendizagem, assegurada a

[27] DA_PT_22 - Escolas visitadas.

[28] DA_26 - Parque dos computadores das escolas visitadas.

diversidade de métodos e propostas pedagógicas, com preferência para softwares livres e recursos educacionais abertos, bem como o acompanhamento dos resultados nos sistemas de ensino em que forem aplicadas.

63. O Programa Nacional de Informática na Educação - ProInfo é um programa educacional com o objetivo de promover o uso pedagógico da informática na rede pública de educação básica. O programa disponibiliza os computadores às escolas públicas do DF exigindo, em contrapartida da SEEDF, a infraestrutura física dos laboratórios de informática e o suporte técnico.

Análises e Evidências

64. Com a finalidade de verificar o uso dos recursos de TIC disponibilizados às escolas do DF para fins educacionais, definiu-se como população-alvo as escolas públicas de ensino infantil, fundamental e médio ligadas à SEEDF, localizadas em áreas urbanas/rurais do DF, excluídas as escolas técnicas por possuírem características singulares.

65. Assim, selecionou-se aleatoriamente as escolas a serem visitadas dentro da população-alvo, levando-se em conta as escolas que possuem laboratórios de informática (Censo 2017) e a Diretoria Regional de Ensino – DRE/SEDF a qual se encontra vinculada, com a finalidade de assegurar que a amostra selecionada fosse representativa.

66. Nesse sentido, visitou-se 31 escolas[29], representando 5% de cada Regional de Ensino do DF.

67. Cabe registrar que o parque de computadores dos laboratórios de informática das escolas do DF foi fornecido pelo ProInfo - Programa Nacional de Informática na Educação do Ministério da Educação.

68. Das visitas *in loco*, restou comprovado que 41,7% dos computadores estão em manutenção e 79,1% apresentam mais de dez anos de uso (obsoletos)[30], em razão da dificuldade de reposição de peças que necessitam de manutenção,

[29] DA_PT_22 - Escolas visitadas.

[30] DA_26 - Parque dos computadores das escolas visitadas.

conforme evidências coletadas abaixo:

Foto 1
Laboratório do Centro de Ensino Médio 02 - Gama

Fonte: Visita *in loco* em 08/05/2018.

Foto 2
Laboratório da Escola Classe 06 de Planaltina

Fonte: Visita *in loco* em 21/05/2018.

Foto 3
Laboratório do Centro de Ensino Fundamental Darcy Ribeiro - Paranoá

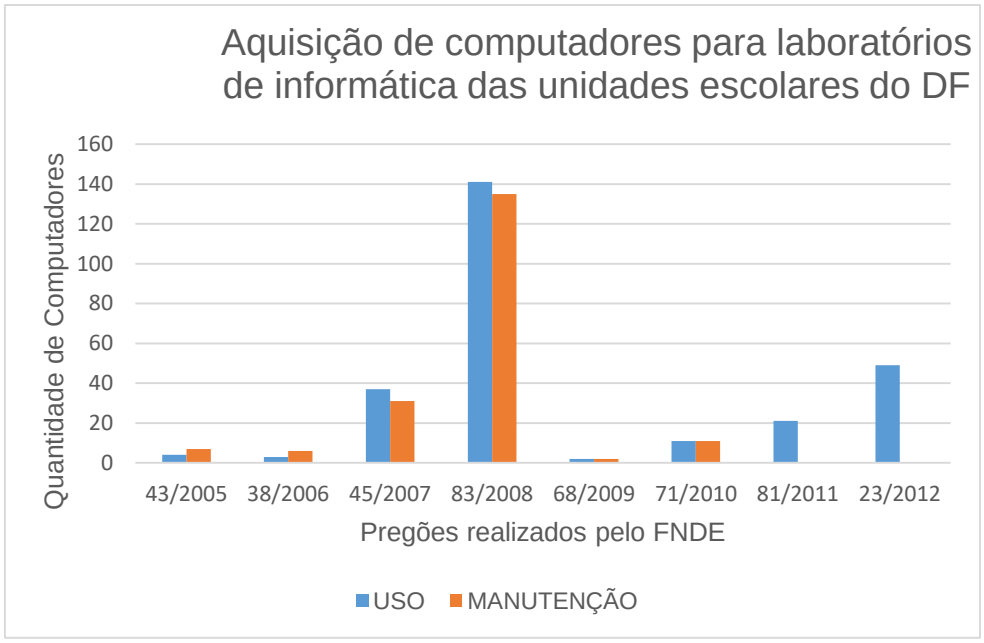
Fonte: Visita *in loco* em 25/04/2018.

Foto 4
Laboratório do Centro de Ensino Fundamental 02 da Estrutural

Fonte: Visita *in loco* em 26/04/2018.

69. O gráfico abaixo, demonstra que os computadores dos laboratórios de informática das escolas do DF foram adquiridos por de meio de licitações realizadas pelo FNDE, no período de 2005 a 2012, o que demonstra a existência de computadores com até 13 anos de vida útil, vejamos:

Gráfico 4



Fonte: Parque de computadores das escolas visitadas (DA_26).

70. Destaca-se que a maioria dos computadores instalados nos laboratórios são oriundos do pregão de 83/2008, ou seja, completando 10 anos de vida útil neste exercício (2018).

71. Sabe-se que o ciclo de vida média dos equipamentos de informática pode variar significativamente (três a oito anos), dependendo do tipo de equipamento (monitor de vídeo/desktop), uso/manutenção e necessidade de atualização tecnológica.

72. Os diretores de escolas entrevistados noticiaram que a empresa contratada pela SEEDF para manutenção dos computadores presta um atendimento satisfatório, identificando e corrigindo os problemas apontados, conforme se verifica na base de chamados, relativa ao período de janeiro de 2018[31].

73. No entanto, quando o diagnóstico da equipe de manutenção se refere à peça danificada ou quebrada, não é possível repô-la, em razão de não ser mais fabricada.

74. Assim, observa-se uma diminuição gradativa dos equipamentos disponíveis por falta de peças de reposição para mantê-los em funcionamento (memória, placa-mãe, entre outros), impactando o uso do laboratório de informática e a consequente oferta de tecnologias (internet, softwares educativos[32]) aos alunos no processo de ensino-aprendizagem.

Causas

75. Carência de recursos financeiros para renovação do parque computacional instalado nos laboratórios de informática das escolas públicas do DF.

Efeitos

76. Impossibilidade de utilizar o computador como ferramenta pedagógica. Ociosidade do laboratório de informática das escolas públicas por falta de equipamentos.

[31] DA_26 - Parque dos computadores das escolas visitadas e arquivo associado ao processo (Listagem de Chamados JANEIRO2018.rar).

[32] As escolas do DF utilizam o Linux Educacional (software livre).

Considerações do Auditado

77. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, assim se manifestou (peça 19, fl. 3):

> *"...A SUMTEC é a área técnica responsável pela elaboração do Plano Diretor de Tecnologia da Informação (PDTI) que norteia as ações necessárias a aquisição e manutenção dos equipamentos e serviços de TI desta SEE/DF. Ao final de 2018 foi concluído o PDTI referente ao período de 2019-2020, o qual aguarda aprovação do Comitê Gestor de TI da Pasta para publicação. Dentre as diretrizes norteadoras do PDTI/SEEDF encontra-se a determinação de renovação do parque tecnológico das unidades escolares em 25% a cada ano. Nesta data, foi finalizado processo licitatório da SEFP. Devendo a SEDF aderir a Ata de Registro de Preços elaborada por aquele órgão (Processo nº 0084-000030/2016). O procedimento foi observado pelo TCDF e aguarda liberação de recursos financeiros do GDF para aquisição dos computadores discriminados. Ressalte-se que parte dos recursos será fornecida pelo Fundo Nacional de Desenvolvimento da Educação (FNDE) e deverá ser, obrigatoriamente, utilizada para aquisição de equipamentos para uso pedagógico, ocasionando consequente renovação do parque computacional instalado nos laboratórios de informática das escolas públicas do DF listadas no processo. Ademais, a SUMTEC tem se colocado em contato constante com outros órgãos do GDF e da esfera federal, além do Poder Judiciário, para celebrar parcerias e/ou obter doações de equipamentos em bom estado que possam substituir máquinas inutilizadas. No que se refere às condições oferecidas pelo Programa Nacional de Informática na Educação (ProInfo), informamos que são disponibilizados computadores, recursos digitais e conteúdos educacionais às escolas públicas, cabendo à SEDF somente o controle de equipamentos instalados e garantia contratual de velocidade do link do maior percentual de banda instalado na área. "*

Posicionamento da equipe de auditoria

78. Apesar de a jurisdicionada noticiar a finalização de procedimento licitatório que irá suprir a demanda pelos equipamentos/computadores, tal medida deverá ser comprovada e seus resultados analisados, razão pela qual mantém-se a proposição apresentada na versão prévia do Relatório de Auditoria.

Proposições

79. Sugere-se ao egrégio Plenário recomendar à SEEDF que:

a. adote as medidas necessárias visando atualizar o parque tecnológico dos laboratórios das escolas públicas do DF, de forma a fomentar o uso dos recursos tecnológicos para melhoria do fluxo escolar e da aprendizagem (meta/estratégia 7.12 do PNE), intensificando, por exemplo, o uso de recursos do Proinfo e celebração de acordos entre órgãos públicos para cessão de equipamentos.

Benefícios Esperados

80. Utilização plena do laboratório de informática, bem assim estímulo ao aluno com o uso de novas tecnologias no processo ensino-aprendizagem.

2.2.2 Achado 4 – baixa velocidade do link de acesso à Internet disponibilizado nos laboratórios de informática das unidades escolares públicas do DF

Critérios

81. A meta/estratégia 7.12 – Tecnologias educacionais do Plano Nacional de Educação – PNE tem o objetivo de incentivar o desenvolvimento, selecionar, certificar e divulgar tecnologias educacionais para a educação infantil, o ensino fundamental e o ensino médio e incentivar práticas pedagógicas inovadoras que assegurem a melhoria do fluxo escolar e a aprendizagem, assegurada a diversidade de métodos e propostas pedagógicas, com preferência para softwares livres e recursos educacionais abertos, bem como o acompanhamento dos resultados nos sistemas de ensino em que forem aplicadas.

82. O Fundo Nacional de Desenvolvimento da Educação - FNDE, por

meio do Programa Banda Larga nas Escolas – PBLE, disponibiliza o acesso à internet para as escolas públicas urbanas do DF.

Análises e Evidências

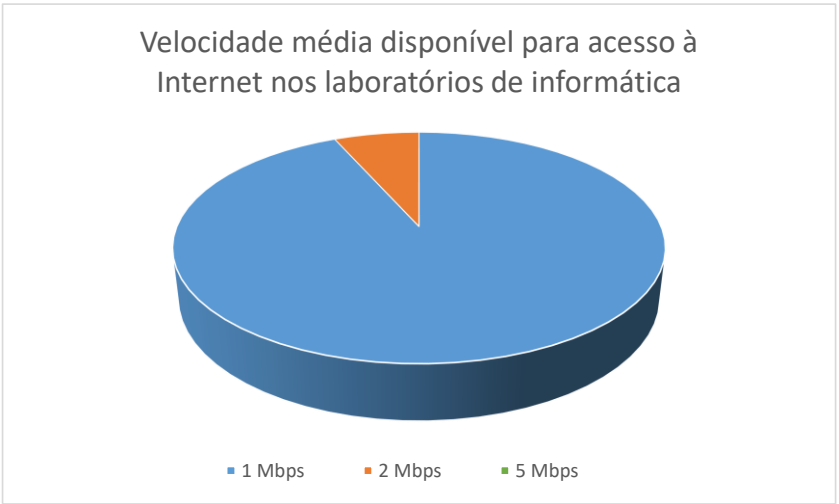
83. Conforme mencionado nos §§67/69 deste relatório, visitas *'in loco'* foram realizadas com a finalidade de avaliar a oferta de TIC nas escolas públicas do DF para fins pedagógicos.

84. Uma das tecnologias verificadas diz respeito à disponibilidade de link de acesso à internet nos laboratórios de informática.

85. Registra-se que o uso da internet como ferramenta educacional pode contribuir com o trabalho pedagógico, auxiliando e ampliando novas competências e metodologias de ensino, razão pela qual os projetos políticos pedagógicos[33] das escolas preveem o uso de internet para atividades em classe, consoante estratégia (7.12) estabelecida pelo PNE.

86. Na maioria das escolas visitadas (90%) verificou-se link de 1 (um) Mbps de velocidade média nos laboratórios de informática das unidades escolares[34], vejamos:

Gráfico 5



Fonte: Arquivo associado ao processo (Escolas visitadas.rar) ou DA_PT_22.

87. Nesse caso, o link disponibilizado pelo Programa Banda Larga nas

[33] PPP's das escolas EC 08 e EC 19 de Taguatinga (Arquivo associado ao processo).

[34] Arquivo associado ao processo (Escolas visitadas) ou DA_PT_22.

Escolas - PBLE é compartilhado pelos alunos que se encontram conectados nos computadores da rede do laboratório de informática, conforme se observa na foto abaixo.

Foto 5
Laboratório da Escola Classe 19 de Taguatinga

Fonte: Visita *in loco* em 02.05.2018.

88. Segundo informações dos diretores de escola, as aulas no laboratório de informática são realizadas com turmas de vinte alunos em média.

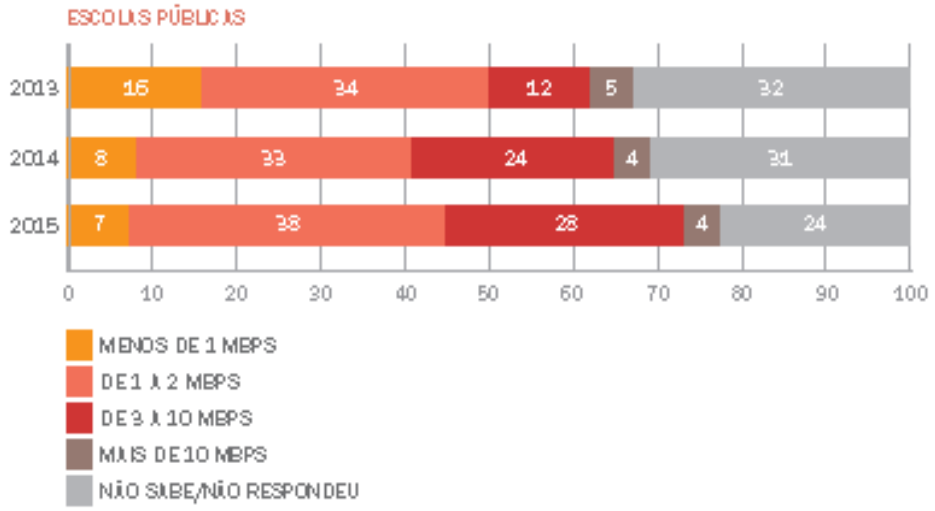
89. Tomando como base esse parâmetro, disponibiliza-se por aluno somente 51,2[35] Kbps[36] a ser consumido nas atividades de pesquisa/navegação de páginas/endereços pela internet.

90. A título comparativo, conforme estudo publicado pela Ookla[37], ferramenta de aferição de velocidade de internet, a velocidade média de acesso à internet fixa no Brasil foi de 17,8 Mbps em 2017, ou seja, quase 18 (dezoito) vezes mais rápido que o link disponibilizado pelo programa PBLE (1 Mbps).

35 1 mpbs / 20 = 1 * 1024 /20 = 51,2 kbps.
36 Taxa de transferência (em kilobit por segundo – Kbps) usualmente utilizada para medir a velocidade da Internet.
37 https://olhardigital.com.br/noticia/velocidade-media-da-internet-aumentou-30-em-2017-brasil-segue-abaixo-da-media/72953. Acessado em 10/08/2018.

91. Em nível nacional, a maioria das escolas públicas brasileiras ainda têm acesso à internet de baixa velocidade (45%), conforme pesquisa realizada sob responsabilidade do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br)[38] em 2015, vejamos:

Gráfico 7
PROPORÇÃO/PERCENTUAL DE ESCOLAS,
POR VELOCIDADE DE ACESSO À INTERNET (2015)



Fonte: Cetic.br, 2015

92. Assim, constata-se baixa velocidade do link de acesso disponibilizado pelo PBLE às escolas públicas do DF, a qual impede a utilização da internet pelos alunos, vez que não é suficiente para atender a quantidade de alunos por turma presentes no laboratório de informática.

93. Tal situação prejudica o aluno, vez que inviabiliza a concretização da proposta pedagógica que contempla o uso dos recursos tecnológicos para a melhoria do processo de aprendizagem, em conformidade com a meta 7.12 – Tecnologias educacionais do PNE - Plano Nacional de Educação.

94. Com efeito, o aluno corre risco de ser prejudicado no seu aprendizado, pois a falta de conectividade impede a integração entre a pedagogia e o uso dos recursos digitais.

[38] Pesquisa sobre o uso de TIC nas escolas brasileiras - TIC Educação 2015. Cetic.br, 2015. Disponível em: < http://cetic.br/media/docs/publicacoes/2/TIC_Edu_2015_LIVRO_ELETRONICO.pdf >. Acessado em 10/08/2018.

Causas

95. Falta de recursos para ampliar a velocidade da Internet disponibilizada nos laboratórios de informática das escolas do DF.

Efeitos

96. Impossibilidade de utilizar a internet como ferramenta pedagógica.

Considerações do Auditado

97. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, assim se manifestou: (peça 19, fls. 3/4)

> *"... O link de acesso à internet destinado as unidades escolares é fornecido pelo Programa Banda Larga nas Escolas (PBLE), lançado pelo governo federal em 4 de abril de 2008, motivo pelo qual não é possível qualquer ingerência relativa a esse serviço por parte da SEEDF. Em 2015, o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS) expediu documento (https://bit.ly/2FFJDDw) em que conclui que as revisões de velocidade que deveriam ocorrer em 2010 e 2013 não foram realizadas e, ainda, não houve sanções por parte da ANATEL às operadoras de telefonia responsáveis. Sendo assim, é possível inferir que o Programa não alcançou os resultados previstos até o momento. Em 2018, o Ministério da Educação forneceu recursos para contratação de conexão de internet por meio do Programa de Inovação Educação Conectada, contemplando 226 unidades escolares por adesão ao programa de destinação de recursos federais PDDE (Programa Dinheiro Direto na Escola). No entanto, as equipes gestoras encontram dificuldades para a contratação haja vista as regras para prestação de contas que exigem orçamentos e certidões que empresas não podem fornecer por motivos diversos. A SEEDF pretende, por meio das metas estabelecidas no Planejamento Estratégico 2019-2022 (#EducaDF), promover a revitalização dos espaços de utilização dos recursos digitais e tecnológicos para o aprendizado, incluindo nesta ação o movimento de links de acesso compatíveis com as atividades demandadas dos estudantes. "*

Posicionamento da equipe de auditoria

98. Verifica-se que a SEEDF pretende adotar medidas efetivas para sanar o problema apontado, uma vez que as soluções disponibilizadas atualmente pela SEEDF para prover os laboratórios das escolas de links de acesso à Internet não atendem satisfatoriamente às demandas estudantis.

99. Desse modo, mantém-se o posicionamento da Equipe de Auditoria apresentado na versão prévia do Relatório de Auditoria.

Proposições

100. Sugere-se ao egrégio Plenário recomendar à SEEDF que:

a. adote as medidas necessárias com a finalidade de aumentar a velocidade média do link de acesso à internet disponibilizada nos laboratórios de informática das escolas do DF, de forma a fomentar o uso dos recursos tecnológicos para melhoria do fluxo escolar e da aprendizagem (meta/estratégia 7.12 do PNE).

Benefícios Esperados

101. Uso de novas tecnologias no processo ensino-aprendizagem.

2.3 Questão 3 - As informações geradas pelos sistemas de gestão escolar e de apoio são confidenciais, íntegras e disponíveis?

As práticas adotadas pela SEEDF, referentes à gestão da segurança da informação encontram-se incipientes, com baixo de nível de maturidade. Além disso, verificou-se expressivo número de demandas represadas do sistema i-Educar (melhorias e/ou defeitos), podendo causar impactos na integridade e disponibilidade do sistema.

2.3.1 Achado 5 – Baixo nível de maturidade de gestão de segurança da informação

Critérios

102. Para análise da segurança da informação dos sistemas de gestão escolar/apoio administrativo da SEEDF foram utilizadas as normas/guias de TIC que se seguem.

103. O modelo COBIT 5, em especial as práticas voltadas para segurança

da informação, e o guia para avaliação de processo "*Process Assessment Model (PAM) using COBIT 5"* (APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança).

104. A ABNT ISO/IEC 27001:2013 é a norma brasileira que trata dos Sistemas de gestão da Segurança da Informação e no item 5.2 trata de forma específica da Política de Segurança da Informação.

105. A ABNT ISO/IEC 27004:2017 é a norma brasileira que trata de monitoramento, medição, análise e avaliação dos sistemas de gestão da segurança da informação e no item 6.5 trata de forma específica de quem irá monitorar, medir, analisar e avaliar.

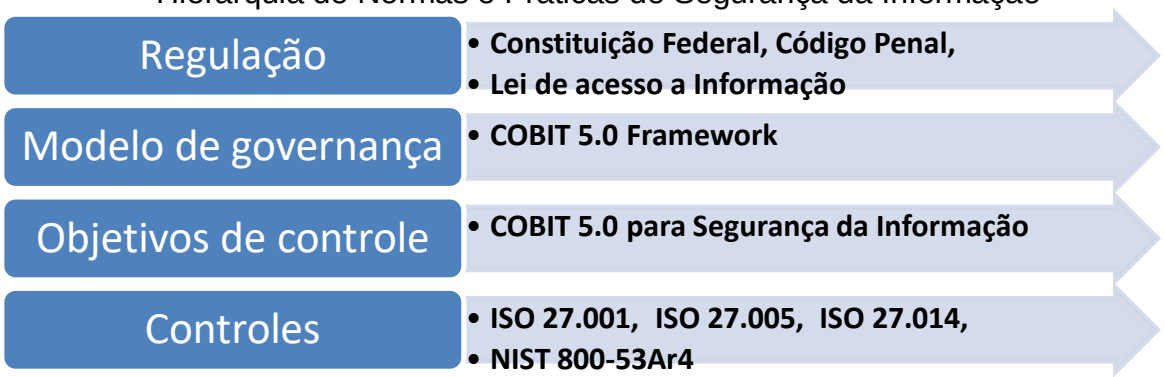
106. A ABNT ISO/IEC 27005:2011 é a norma brasileira que trata dos Sistemas de Gestão de Riscos da Segurança da Informação e no item 8 trata de forma específica do Processo de Avaliação de Riscos de Segurança da Informação e no item 9 do Tratamento de Riscos de Segurança da Informação.

107. A ABNT ISO/IEC 27014:2013 é a norma brasileira que trata da Governança de Segurança da Informação e no item 5.3.3 trata de forma específica do processo "Direção" da Segurança da Informação.

108. A NIST SP 800-53A4 é uma norma que trata de avaliação de controles de segurança e privacidade das organizações e dos sistemas de informação do governo federal americano e caracteriza-se por ser aplicável a qualquer organização. Esta norma foi utilizada para avaliação da Secretaria de Estado de Educação em forma de questionário em nota de auditoria.

109. A figura a seguir permite identificar qual a predominância de normas e modelos utilizados neste achado.

Figura1
Hierarquia de Normas e Práticas de Segurança da Informação



Análises e Evidências

110. A implementação da segurança da informação inclui não apenas os sistemas de informação, mas também qualquer forma de informação armazenada que tenha valor para organização ou indivíduos.

111. A segurança da informação tem relevância internacional o que levou a elaboração de diversos modelos e práticas já consolidados internacionalmente para proteção da informação e comumente considerados como as melhores práticas de mercado que objetivam a eficiência e melhor retorno dos investimentos e proteção às organizações.

112. O objetivo de um sistema de gestão de segurança da informação é preservação da confidencialidade, integridade e disponibilidade das informações.

113. O "COBIT 5 para Segurança da Informação" define segurança da informação como algo que garante que, dentro da empresa, as informações sejam protegidas contra divulgação a usuários não autorizados (confidencialidade), modificação indevida (integridade) e acesso quando necessário (disponibilidade).

- ✓ Confidencialidade significa preservar as restrições autorizadas de acesso e divulgação, incluindo meios para proteger a privacidade e informações proprietárias;
- ✓ Integridade significa proteção contra modificação ou destruição indevida de informações e inclui garantia de não-repúdio e autenticidade;
- ✓ Disponibilidade significa garantir acesso e uso oportuno e confiável de informações.

114. Esses três princípios da segurança da informação serão tratados neste achado, considerando também as condições de contexto necessárias para sua existência na Tecnologia da Informação, como governança e gestão.

115. No âmbito da Administração Pública do DF, existe um Centro de Processamento de Dados (*Datacenter*) na Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do DF (SEFP) que compartilha o uso de recursos computacionais com diversas outras secretarias de estado, dentre elas, a SEEDF.

116. Os sistemas informatizados da SEEDF estão hospedados neste datacenter da SEFP com algumas redundâncias de dados em outro datacenter da

mesma Secretaria.

117. As evidências constantes deste tópico estão presentes nas respostas[39] às Notas de Auditoria nºs 02 e 03 – 4093/2018, doravante mencionadas como Nota nº 2 e Nota nº 3, respectivamente (DA nº 30 e 18).

118. A Nota nº 03 – 4093/2018 contém 139 questões com base no documento para avaliação de controles de segurança e privacidade das organizações e dos sistemas de informação NIST SP 800-53A4. As demais notas de auditoria também abordam algumas questões específicas relativas a este achado.

119. A seguir, apresentam-se as análises por temática.

Política e práticas de Segurança da Informação

120. Consoante respostas às notas de auditoria expedidas neste trabalho, os documentos destinados a viabilizar a política ou prática de segurança de informação ou não existem ou estão em revisão, o que reflete a ausência de política de segurança de informação formalizada, conforme respostas a seguir:

- ✓ política de acesso está sob revisão (questão 1, nota nº 2);
- ✓ política de autorização de acesso (inexiste) (questão 24, nota nº 3);
- ✓ política de segurança de configuração (inexiste) (questão 27, nota nº 3);
- ✓ política de plano de contingência (inexiste) (questão 35, nota nº 3);
- ✓ política de identificação e autenticação (inexiste) (questão 47, nota nº 3);
- ✓ política de resposta à incidentes (inexiste) (questão 64, nota nº 3);
- ✓ política de manutenção (existe) (questão 81, nota nº 3);
- ✓ política ou procedimentos de proteção de mídia documentado (inexiste) (questão 89, nota nº 3);
- ✓ política de proteção física e do ambiente (é feita pela Seplag) (questão 95, nota nº 3);
- ✓ política de planejamento de segurança (conforme o PosiC do GDF[40]) (questão 107, nota nº 3);

[39] Arquivos associados ao processo (NotaAud02_08_P4093_18RespostaSUMTEC.pdf e NotaAud03_08_P4093_18RespostaSUMTEC.pdf) ou DA_30 e DA_18.

[40] http://www.seplag.df.gov.br/wp-conteudo/uploads/2017/10/PoSIC_GDF.pdf

- ✓ política de avaliação de risco (inexiste) (questão 129, nota nº 3).

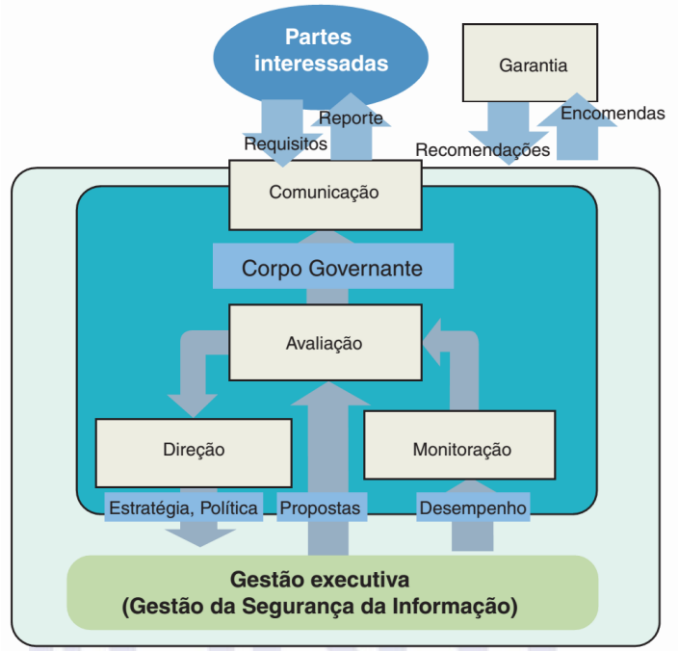
121. O atual cenário da SEEDF é de quase inexistência de documentação que permita estabelecer as diretrizes de segurança de informação.

122. A ausência de política de segurança dificulta a boa governança e a gestão da segurança da informação resultando no aumento de riscos para as organizações.

123. Segundo o item 5.3.3 da ISO 27014, que normatiza a governança de segurança da informação, o processo de "Direção" envolve o desenvolvimento e a implementação da Política de Segurança da Informação (PSI) pela gerência executiva[41] das instituições.

124. A PSI é essencial para implementação de governança de segurança da informação, pois define os papéis e responsabilidades das partes envolvidas. A figura a seguir apresenta esse modelo e identifica os elementos necessários.

Figura 2
Implementação do modelo de governança
para segurança da informação – ISO 27014



Fonte: ISO 27014.

125. O escopo da governança da segurança da informação abrange a

[41] Gerência Executiva - Pessoa ou grupo de pessoas que possuem responsabilidade delegada pelo corpo diretivo para a implementação de estratégias e políticas para alcançar o propósito da organização. Corpo Diretivo - pessoa ou grupo de pessoas, que são responsáveis pelo desempenho e conformidade da organização ISO 27014:2013.

confidencialidade, integridade e disponibilidade da informação, tratados pelos seguintes processos de governança: Avaliação, Direção e Monitoração e pelo processo interno de “comunicação”, que são atribuições da governança, e portanto, da alta administração da instituição.

126. Outra norma de segurança da informação, a ISO 27.001, define que o objetivo da política de segurança da informação é prover orientação do processo de direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

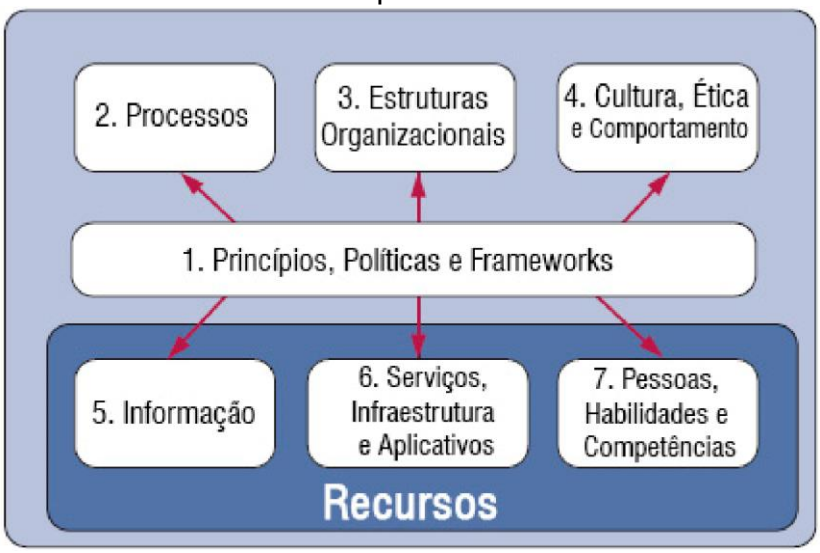
127. A ISO 27.001 também estabelece que a política de segurança da informação deve:

- ✓ Estar disponível como informação documentada;
- ✓ Ser comunicada dentro da organização;
- ✓ Estar disponível para as partes interessadas, conforme apropriado.

128. A ausência de políticas de segurança da informação transparente e bem definida representa fator de risco considerável à organização pois não estabelece controles adequados ao acesso de links, e-mails e sites, e também a devida orientação e treinamento aos usuários internos e externos dos sistemas.

129. Sob o ponto de vista do modelo COBIT 5 para Segurança da Informação, a política é considerada um habilitador essencial que traduz o comportamento desejado de orientações práticas para gestão diária.

Figura 3
Habilitadores corporativos do COBIT 5



Fonte: COBIT 5.

130. Outro aspecto relevante da ausência de política de segurança formalizada, é a falta de definição do que pode ser considerado como gestão de segurança da informação e a atividade para manutenção da segurança da informação.

131. Essa diferenciação é relevante pois, a Instrução Normativa SLTI nº 04/2014 (recepcionada pelo decreto 37.667/16) veda a contratação de gestão de segurança da informação, vejamos:

> *"Instrução Normativa SLTI n° 4, de 11.09.14.*
> *Art. 5º Não poderão ser objeto de contratação:*
> *(...) II - gestão de processos de Tecnologia da Informação, incluindo gestão de segurança da informação."*

132. No caso da SEEDF, a empresa Stefanini executa o monitoramento contínuo da Segurança da Informação, conforme resposta à pergunta 25 da Nota nº 3, situação em que a política de segurança da informação deveria atuar como definidor das atividades e competências de cada agente e seu papel, mas que se torna prejudicada pela inexistência de formalização da política.

133. Outra característica importante nesse contexto é o fato de as informações presentes no sistema i-Educar alimentarem o sistema do DFTRANS para o benefício do passe livre estudantil, o que eleva os riscos do sistema e, consequentemente, os requisitos de segurança da solução, pois, além de tratar da gestão acadêmica, assegura benefícios aos estudantes que repercutem

financeiramente para o Estado (ver Processo TCDF nº 31.428/2017[42]).

134. Nesse contexto, faz-se necessário determinar à SEEDF que elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27014:2013).

Identificação e acesso (Questões de 47 a 63 da Nota nº3)

135. Em que pese a criticidade do sistema i-Educar para a gestão escolar, verificou-se que a forma de autenticação existente nos sistemas I-Educar e Sigep é efetuada por usuário e senha (máximo de oito caracteres, bloqueio no caso de três erros sucessivos e renovação periódica) o que representa um baixo nível de segurança, pois contempla apenas um fator de autenticação mais vulnerável do que outros métodos, a exemplo da autenticação única por certificação digital (questão nº 48, Nota nº 3).

136. A forma de autenticação com um único fator adotada pela SEEDF nos sistemas i-Educar e no Sigep representa uma vulnerabilidade que pode ser explorada por ameaças, e pode causar danos aos ativos da organização, como alteração de informações, representando perda de confidencialidade e integridade dos sistemas.

137. Desse modo, entende-se cabível determinar à SEEDF que tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso aos sistemas críticos, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT ISO 27.001 e ABNT ISO 27.005.

Gerenciamento de riscos em Segurança da Informação (questões nºs 129 a 132

[42] Auditoria Integrada - Segurança da Informação no Sistema de Bilhetagem Automática

da nota 3)

138. Em resposta à Nota de Auditoria nº 3[43], a jurisdicionada informou que não há política ou procedimento de avaliação de riscos (questão nº 129), expressou que não há estratégia de gerenciamento de riscos (questão nº 116) e que também não foi realizada uma avaliação de risco de acesso não autorizado que venha a modificar, destruir, alterar ou divulgar informações (questão nº 130).

139. A principal função do gerenciamento de riscos na Segurança da Informação é fornecer confiança às partes interessadas de que os riscos são adequadamente gerenciados para melhor preservar a confidencialidade, integridade e disponibilidade da informação.

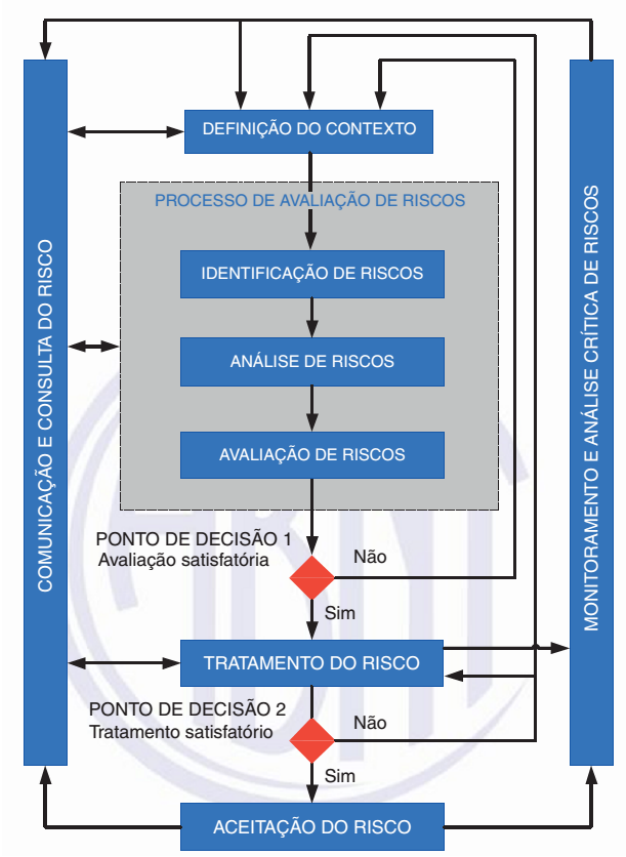
140. Os sistemas em exame (i-Educar e SiGEP) são acessados por meio da internet que se encontra em ambiente hostil[44], o que eleva os riscos a que a SEEDF está exposta e, portanto, torna necessário reavaliações periódicas dos níveis de riscos e respectivas medidas de tratamento de riscos (ISO 27001 e ISO 27005).

141. Desse modo, o gerenciamento de riscos é parte integrante do processo de Segurança da Informação e na ISO 27005 estabelece-se o fluxo do processo de gestão de riscos de segurança da informação, a seguir apresentado.

[43] DA nº 18.

[44] As ameaças mais comuns da internet. Acesso em 15.08.18. < http://www.mundodoshackers.com.br/as-ameacas-mais-comuns-da-internet>

Figura 4
Processo de gestão de riscos de segurança da informação (ISO 27005).



Fonte: ISO 27005.

142. A ISO 27014 estabelece como um dos princípios específicos para governança da segurança da informação a adoção de uma abordagem baseada em riscos.

143. Nesse contexto, sugere-se determinar à SEEDF que passe a adotar abordagem baseada em riscos para Segurança da Informação em conformidade com as normas ABNT ISO 27.001, ISO 27.005, ISO 27.014.

Maturidade do Processo de Segurança da Informação

144. Segundo preconiza a ABNT ISO 27001, a segurança da informação deve ser tratada como um processo cíclico nos moldes do PDCA (do inglês: *PLAN - DO - CHECK - ACT ou Adjust*) que é um método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos.

145. O modelo do COBIT 5 define 37 processos para governança e gestão de TI, e desses, três são descritos para segurança da informação como guia básico

para definir, operar e monitorar um sistema geral de gerenciamento de segurança, a saber: APO13 – Gerenciar Segurança, DSS04 – Gerenciar continuidade e DSS05 – Gerenciar serviços de segurança.

146. O modelo do COBIT 5 define a maturidade do processo por seis níveis de capacidade a seguir descritos: 0 Processo Incompleto; 1 Processo Executado; 2 Processo Gerenciado; 3 Processo Estabelecido; 4 Processo Previsível e 5 Processo Otimizado.

147. Para identificar em que nível de capacidade se enquadram os três processos mencionados anteriormente, que delineiam a segurança da Informação, o COBIT 5 apresenta um documento específico, *Process Assessment Model (PAM) using COBIT 5*, que detalha as atividades que devem ser executadas para ser considerado em cada nível.

148. A Tabela a seguir identifica as práticas de cada processo de gerenciamento de riscos executadas pela SEEDF:

Tabela 4

Critérios para avaliação do alcance de resultados para o nível de maturidade 1 - Processo Executado		
Os seguintes resultados do processo estão sendo alcançados?	Alcance*	evidências: respostas da Nota 3
APO13 – Gerenciar Segurança		
APO13-01 Um sistema em uso que efetivamente aborda os requisitos de segurança de informações corporativas.	PA	Q 24/26
APO13-02 Um plano de segurança foi estabelecido, aceito e comunicado em toda a empresa.	NA	Q 111/112
APO13-03 As soluções de segurança da informação são implementadas e operadas de forma consistente em toda a organização.	PA	Q 113 e 139
DSS04 – Gerenciar continuidade		
DSS04-01 As informações críticas de negócios estão disponíveis para os negócios de acordo com os níveis mínimos de serviço necessários.	PA	Q 46/80
DSS04-02 Resiliência suficiente está em vigor para serviços críticos.	PA	Q 70/75
DSS04-03 Testes de continuidade de serviço verificaram a eficácia do plano.	NA	Q 67
DSS04-04 Um plano de continuidade atualizado reflete os requisitos de negócios atuais.	NA	Q 72
DSS04-05 Partes internas e externas foram treinadas no plano de continuidade.	NA	Q 35, 64 e 72
DSS05 – Gerenciar serviços de segurança		
DSS05-01 A segurança de redes e comunicações atende às necessidades de negócios.	AA	Q 95/106 e 133/137
DSS05-02 As informações processadas, armazenadas e transmitidas pelos dispositivos de rede da ponta estão protegidas.	PA	Q 24/26 e 47/63
DSS05-03 Todos os usuários são exclusivamente identificáveis e possuem direitos de acesso de acordo com sua função de negócios.	AA	Q 47/63
DSS05-04 Medidas físicas foram implementadas para proteger informações contra acesso não autorizado, dano e interferência ao serem processadas, armazenadas ou	AA	Q 95/106
DSS05-05 A informação eletrônica é adequadamente protegida quando armazenada, transmitida ou destruída.	AA	Q 37, 42/46 83/84, 92/93, 130

Nota: *Alcance: NA - Não Alcançado (0-15%), PA - Parcialmente Atingido (15% -50%), AA - Amplamente atingido (50% - 85%) ou TA - Totalmente Atingido (85-100%).
Fonte: Nota de Auditoria nº 03-4093/2018 e *Process Assessment Model (PAM) using COBIT 5.*

149. Consoante a tabela acima, verifica-se que a Secretaria não executa a integralidade das práticas de cada processo de segurança da informação para alcançar o nível de capacidade 1 (um - processo executado), indicando assim que os processos de segurança da informação da SEEDF possuem nível de capacidade 0 (zero - incompleto).

150. Nesse sentido, cabe determinar à SEEDF a melhoria contínua dos processos e produtos de segurança da informação, de acordo com as boas práticas (APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança do COBIT 5.0).

Termos de Responsabilidade

151. Em resposta a Nota de Auditoria nº 3, a jurisdicionada informou que não existe termo de responsabilidade para acesso aos sistemas (questão 10).

152. Cabe mencionar a importância da cientificação de cada usuário de suas atribuições e responsabilidades legais, bem como as possíveis ameaças que possam causar impacto danoso à informação da SEEDF.

153. Desse modo, os servidores devem pôr a termo a sua ciência das implicações de uso indevido dos sistemas, assim como é exemplificado no termo de responsabilidade de acesso ao SIGGO[45] e de outros sistemas do GDF.

154. Nesse sentido, cabe determinar à SEEDF que elabore e faça uso de termo que cientifique os usuários dos sistemas quanto as suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos assinados pelos usuários.

Gerenciamento de Acesso de Usuários (questões nºs 5 e 123 da Nota nº 3)

155. Um grave problema de segurança da informação é quando um servidor ou usuário do sistema deixou o cargo ou apresentou suas atribuições modificadas e seu acesso ainda permanece ativo nos sistemas, que muitas vezes incluem a possibilidade de alteração de dados e/ou realização de consultas de caráter restrito / sigiloso.

156. Como exemplo de solução para essa falha, os sistemas de recursos humanos, quando do ingresso dos servidores à organização, apresentam junto com sua inclusão administrativa a possibilidade de criação de autorizações de acesso específicas ao cargo e, caso o servidor venha a assumir atribuições administrativas diferentes, as alterações das funções administrativas no sistema de RH passam a ser refletidas nas autorizações de acesso aos sistemas e, ainda, na possibilidade da saída definitiva do órgão, o sistema de RH deve efetivar ou iniciar a revogação de acessos de forma imediata em todos os sistemas da organização.

157. No caso da SEEDF, a Subsecretaria de Gestão de Pessoas, que é responsável pelo ingresso e gestão dos servidores da SEEDF, efetiva a parte

[45] Disponível em www.fazenda.df.gov.br.

administrativa e encaminha à Subsecretaria de Modernização e Tecnologia para alteração de perfil de acesso conforme o caso, ou até o bloqueio de acesso para os que deixaram de exercer atividades no âmbito da SEEDF.

158. Caso essa comunicação não ocorra ou demore a acontecer, o acesso permanece por tempo indevido, representando grave risco à segurança da informação da SEEDF (questões nºs 5, 6, 123 e 124 da Nota nº 3).

159. O sistema de gerenciamento de pessoal do DF, SIGRH, é um sistema antigo com muitas deficiências e de difícil manutenção que está em processo de substituição no GDF[46], o que torna inviável, no momento, a implementação da funcionalidade descrita anteriormente.

160. No entanto, existe uma possibilidade para mitigação do risco envolvido no acesso de quem não deveria mais possuí-lo. Entende-se que aquele que tem a atribuição de efetivar administrativamente as alterações de cargos na SEEDF também deveria efetivar a alteração de perfil de acesso aos sistemas da SEEDF, via perfil específico, que pode ser criado pela Subsecretaria de Modernização e Tecnologia no AD (*Active Directory*) e demais sistemas que realizem as autenticações dos servidores para acesso aos sistemas.

161. Desse modo, uma das alternativas para mitigação do risco é a Subsecretaria de Gestão de Pessoas, que atualmente faz a gestão administrativa de pessoal, também realizar a gestão de acesso de sistemas dos servidores da SEEDF, reduzindo as possibilidades de acesso indevido, até que novo sistema de pessoal do GDF possa espelhar automaticamente os papéis e responsabilidades dos servidores com os perfis de acesso aos sistemas de informação.

Causas

162. Inobservância das boas práticas dos processos de segurança da informação.

Efeitos

163. Melhoria da gestão de segurança da informação.

[46] Processo licitatório acompanhado por este TCDF – Processo nº 58/2017

Considerações do Auditado

164. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, assim se manifestou: (peça 19, fls. 4/6)

".Achado 5 - Baixo nível de maturidade de gestão de segurança da informação

Para elaboração do Relatório Prévio de Auditoria ora apresentado, as equipes gestoras das áreas técnicas responsáveis responderam a questionários apresentados pelos Auditores de Controle Interno. Diante das respostas fornecidas, os mesmos indicam as recomendações que serão submetidas ao Plenário, às quais fazemos referência para informar quanto às ações em curso no âmbito desta Subsecretaria para a observância de boas práticas dos processos de segurança da informação:

1) (...) será submetida à deliberação do egrégio Plenário, ao menos, a seguinte proposição:

II. Determinar à Secretaria de Estado de Educação que:

a) elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27014:2013);

(...) c) passe a adotar abordagem baseada em riscos para segurança da informação conforme estabelece a ISO 27.001, ISO 27.005 e ISO 27.014;

A Política de Segurança da Informação da SEEDF (PoSIC/SEEDF está prevista no PDTI 2019-2020 e encontra-se em fase final de elaboração. Será publicada e divulgada no 1º Semestre de 2019.

2) b) tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso aos Sistemas de Tecnologia da Informação considerados críticos, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ISO ABNT 27.001 e ABNT ISO 27.005;

(...) d) elabore e faça uso de termo que cientifique os usuários dos sistemas quanto as suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos

assinados pelos usuários;

Os sistemas sustentados pela SUMTEC possuem duas formas de acessos: por validação por meio do Active Directory(AD) e por cadastro do CPF, realizado pelo responsável conforme perfil.

A Diretória de Governança em TI incluiu na PoSIC/SEEDF modelos de Termos de Responsabilidade e Confidencialidade para uso dos sistemas, os quais serão disponibilizados aos usuários internos após automatização realizada pela Diretória de Desenvolvimento de Sistemas.

Os usuários externos devem preencher Termo de Confidencialidade para acesso ao i-Educar.

> *3) (...) e) promova a melhoria contínua dos processos e produtos de segurança da informação, de acordo com as boas práticas (AP013 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança do COBIT 5.0).*
>
> *f) implante sistema automatizado de gestão de acessos e autorizações aos sistemas i-Educar e Sigep, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma que a gestão administrativa de pessoal opere de forma integrada e consistente com a gestão de acesso de sistemas pelos servidores da SEEDF.*

A SUMTEC tem envidado esforços no sentido de promover capacitação e estruturação na área de governança de TI, a fim de alcançar o nível de maturidade desejável à segunda maior secretaria de estado do DF, motivo pelo qual solicitou a aquisição de cursos preparatórios na área e tem fomentado a troca de experiências entre os órgãos públicos.

Da mesma forma, esta área administrativa buscará iniciar ação conjunta com a Subsecretaria de Gestão de Pessoal a fim de estabelecer protocolo para gerenciamento do banco de servidores usuários dos sistemas, seus locais de exercício e níveis de permissão. Nesta data, o sistema de monitoramento existente necessita de melhoramentos e automatização, processo que se encontra em curso.".

Posicionamento da equipe de auditoria

165. A jurisdicionada informou que a política de segurança da informação

da SEEDF está em fase de elaboração. Também adita que envidou esforços em promover capacitação e estruturação na área de governança de TI para melhorar o nível de maturidade da Secretaria. Por fim, informou que que atuará em conjunto com a Subsecretaria de Pessoal a fim estabelecer protocolo para gerenciamento do banco de servidores usuários dos sistemas.

166. Estas são algumas ações necessárias para o início de uma implementação de segurança da informação na Secretaria, no entanto, ainda não foram implementadas e não são suficientes ao atendimento das sugestões de melhoria da segurança de informação para SEEDF.

167. Desse modo, mantém-se inalterado o posicionamento da Equipe de Auditoria apresentado na versão prévia do Relatório de Auditoria.

Proposições

168. Sugere-se ao egrégio Plenário determinar à Secretaria de Estado de Educação que:

a. elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27014:2013);
b. tome as medidas necessárias para melhorar a segurança do processo de identificação e acesso aos Sistemas de Tecnologia da Informação considerados críticos, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT ISO 27.001 e ABNT ISO 27.005;
c. passe a adotar abordagem baseada em riscos para segurança da informação conforme estabelece a ISO 27.001, ISO 27.005 e ISO 27.014;
d. elabore e faça uso de termo que cientifique os usuários dos sistemas quanto as suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos assinados pelos usuários;
e. promova a melhoria contínua dos processos e produtos de segurança da informação, de acordo com as boas práticas (APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança

do COBIT 5.0).

f. implante sistema automatizado de gestão de acessos e autorizações aos sistemas i-Educar e Sigep, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma que a gestão administrativa de pessoal opere de forma integrada e consistente com a gestão de acesso de sistemas pelos servidores da SEEDF.

Benefícios Esperados

169. Melhoria no processo de segurança da informação pelas partes interessadas (todos os envolvidos direta e indiretamente) e redução dos riscos de danos às informações da SEEDF.

2.3.2 Achado 6 – Capacidade insuficiente de a SEEDF atender às demandas do Sistema i-Educar

Critérios

170. COBIT 5, BAI03.03 – Desenvolver componentes da solução; BAI03.05 – Construir soluções; BAI09 - Gerenciar ativos de TI.

Análises e Evidências

171. O Sistema i-Educar é um software de gestão escolar disponibilizado no Portal do Software Público Brasileiro[47], em 2008, por meio de um sistema com banco de dados centralizado e totalmente *web*.

172. A principal finalidade do software é informatizar a gestão das informações educacionais, contribuindo com a racionalização do trabalho.

173. No âmbito da SEEDF, o i-Educar foi formalizado por meio da Portaria nº 29, de 13 de fevereiro de 2014, a qual determinou a utilização plena do sistema para escrituração acadêmica em todas as unidades escolares.

174. As demandas de manutenção e/ou melhoria executadas no sistema i-Educar tem como finalidade a implementação/alteração de funcionalidades, levando-se em conta as necessidades do negócio, de acordo com as melhores práticas de

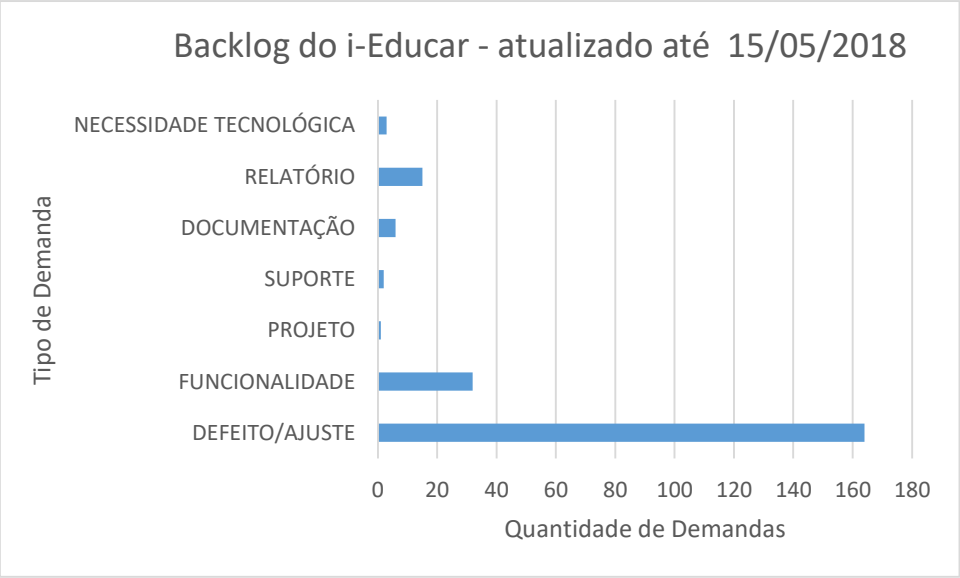
[47] https://softwarepublico.gov.br/social/i-educar

mercado (COBIT 5, BAI03.03, BAI03.03 e BAI09).

175. Cabe registrar que o sistema i-Educar é manutenido/atualizado por equipe própria da área de sistemas da SEEDF desde a sua implantação na rede escolar (2014). Essa equipe é formada por oito servidores que realizam as atividades de análise e programação de sistemas, segundo informações do coordenador da equipe.

176. Em atendimento à Nota de Auditoria nº 04-4093/2018, a SEEDF disponibilizou relatório[48] das demandas represadas (backlog[49]) do sistema i-Educar, atualizado até o dia 15.05.18, considerando os tipos de serviços a serem executados, vejamos:

Gráfico 8



Fonte: *Backlog* i-Educar.

177. O gráfico acima, demonstra um total de 223 demandas abertas até 15/05/2018 do sistema i-Educar, evidenciando um alto risco de a SEEDF não conseguir atender a essas demandas pela equipe atualmente alocada para manter o sistema, considerando que aproximadamente 51% das demandas (113), tem prioridade urgente, alta e imediata.

178. Ainda, observa-se quantitativo expressivo de demandas para

[48] Arquivo associado ao processo (01_201805151149_backlog_ieducar.pdf).

[49] Refere-se a um log (resumo histórico) de acumulação de trabalho num determinado período de tempo.

correção de defeitos ou ajustes (164), as quais necessitam de alocação de recurso tempestivo para atendimento, impactando, assim, a execução das demandas de melhorias do sistema (novos projetos/funcionalidades).

Causas

179. Falta de priorização da gestão do projeto. Falta de pessoal especializado.

Efeitos

180. Potencial risco de não atender às demandas do sistema i-Educar. Não implementar melhorias capazes de otimizar a gestão escolar.

Considerações do Auditado

181. A SEEDF, por meio do Ofício SEI-GDF nº 635/2019 - SEE/GAB, assim se manifestou: (peça 19, fls. 6)

> *"...Esta Secretaria de Educação conta hoje com reduzido quadro de servidores especializados em desenvolvimento de sistemas, seja pela ausência de contratação para o quadro de pessoal, seja pela volatilidade existente no mercado de trabalho de TI. Desta forma, os recursos humanos disponíveis para atendimento das demandas são escassos.*
>
> *A Subsecretaria de Modernização e Tecnologia-SUMTEC iniciou processo licitatório para contratação de serviços de Fábrica de Software, de modo a suprir a escassez de mão de obra especializada na área, além de ação de revisão de processos junto à área de negócios responsável pelo i-Educar, a fim de reexaminar possíveis gargalos existentes na solução das demandas.*
>
> *Ainda, em referência a gestão do i-Educar, a Diretória de Desenvolvimento de Sistemas da SUMTEC pretende capacitar os servidores para adoção de metodologia ágil (SCRUM) no gerenciamento das demandas encaminhadas à área. ".*

Posicionamento da equipe de auditoria

182. Apesar de a jurisdicionada noticiar procedimento licitatório que irá suprir a demanda pelos serviços de fábrica de software, tal medida deverá ser comprovada e seus resultados analisados, até porque o processo[50] ainda se encontra na fase de pesquisa de preços, conforme contato telefônico realizado com a Secretaria de Educação.

183. Nesse sentido, mantém-se a proposição apresentada na versão prévia do Relatório de Auditoria.

Proposições

184. Sugere-se ao egrégio Plenário a proposição de recomendar à SEEDF que:

a. adote medidas administrativas capazes de reestabelecer o fluxo normal de atendimento das demandas represadas, em conformidade com as melhores práticas de mercado (COBIT 5, BAI03.03, BAI03.03 e BAI09), vez que o atual ritmo pode comprometer a correção de defeitos e/ou melhorias do sistema i-Educar.

Benefícios Esperados

185. Diminuição do *backlog* atualmente existente do sistema i-Educar. Atendimento tempestivo das demandas.

3 Conclusão

186. A presente auditoria integrada foi realizada na Secretaria de Estado de Educação do Distrito Federal – SEEDF, em cumprimento ao PGA 2018, tendo como objeto os principais recursos de tecnologia da informação e comunicação (TIC) disponibilizados pela SEEDF no suporte ao ensino educacional do DF, a segurança da informação dos sistemas de gestão escolar e a execução dos principais contratos de informática da SEEDF.

187. Os resultados da auditoria demonstraram que a maioria dos computadores dos laboratórios de informática das escolas públicas do DF (79,1%)

[50] Processo SEI nº 0080.00066779/2018-75.

possui mais de dez anos de uso (obsolescência), o que compromete a utilização dos recursos de TIC e o uso de novas tecnologias pelo aluno no processo ensino-aprendizagem.

188. Além disso, a baixa velocidade do link de acesso disponibilizado nos laboratórios de informática não permite a utilização da Internet pelos alunos, o que inviabiliza a concretização da proposta pedagógica que contempla o uso dos recursos tecnológicos para a melhoria do processo de aprendizagem, nos termos da meta 7.12 – Tecnologias educacionais do PNE - Plano Nacional de Educação.

189. Quanto à gestão da segurança da informação realizada pela SEEDF verificou-se baixo nível de maturidade que compromete a confidencialidade, integridade e disponibilidade das informações.

190. Verificou-se, também, a necessidade de a SEEDF atender o excesso de demandas acumuladas do sistema i-Educar, sob pena de impactar o processo de gestão escolar realizado pelas unidades da rede pública.

191. No que diz respeito a regularidade dos Contratos nºs 19/2013 (fornecimento de circuito de dados) e 06/2016 (suporte técnico) verificou-se a descontinuidade dos serviços de enlace de comunicação de dados nas unidades educacionais e o elevado índice de atendimento presencial, respectivamente.

4 Proposições

192. Ante o exposto, sugere-se ao Plenário:

I. recomendar à Secretaria de Educação do DF que:

a) implemente ações no sentido de estabelecer procedimentos/roteiros com regras pré-determinadas para resolução imediata de incidentes pelo Service Desk (Central de Serviços), de forma a reduzir as ocorrências de escalonamento de incidentes/demandas de usuários, em conformidade com o ITIL – gestão de incidentes e COBIT DS8, bem como mecanismos de controle que permitam o monitoramento dos serviços prestados, nos termos do o art. 20 da IN 04/2014-SLTI/MPOG;

b) adote as medidas necessárias visando atualizar o parque

tecnológico dos laboratórios das escolas públicas do DF, bem como o aumento da velocidade média do link de acesso à internet, de forma a fomentar o uso dos recursos tecnológicos para melhoria do fluxo escolar e da aprendizagem (meta/estratégia 7.12 do PNE), intensificando, por exemplo, o uso de recursos do Proinfo e celebração de acordos entre órgãos públicos para cessão de equipamentos;

c) reestabeleça o fluxo normal de atendimento das demandas represadas do sistema i-Educar, em conformidade com as melhores práticas de mercado (COBIT 5: BAI03.03, BAI03.03 e BAI09), uma vez que o atual ritmo pode comprometer a correção de defeitos e/ou melhorias do sistema i-Educar;

II. determinar à Secretaria de Educação que adote as seguintes medidas, informando ao Tribunal, no prazo de 60 (sessenta) dias, as providências adotadas e resultados alcançados:

a) implemente ações de contingência eficazes para suprir a carência de acesso à internet pelas unidades escolares, considerando a ineficácia do PDAF como opção de contingência, nos termos do artigo 13, inciso V, a IN SLTI MPOG nº 04/2014;

b) elabore, divulgue e utilize sua Política de Segurança da Informação e, quando necessário, os normativos dela derivados (ex: procedimentos de Controle de Acesso Lógico e Físico, Cadastramento de Usuários etc.), conforme as boas práticas de segurança da informação (COBIT 5, ABNT ISO 27001:2013, ABNT ISO 27014:2013);

c) implemente ações para melhorar a segurança do processo de identificação e acesso aos Sistemas de Tecnologia da Informação considerados críticos, de forma a assegurar níveis de risco aceitáveis, nos termos das normas ABNT ISO 27.001 e ABNT ISO 27.005;

d) passe a adotar abordagem baseada em riscos para segurança da informação conforme estabelece a ISO 27.001, ISO 27.005 e ISO

27.014;

e) elabore e faça uso de termo que cientifique os usuários dos sistemas quanto as suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos assinados pelos usuários;

f) promova a melhoria contínua dos processos e produtos de segurança da informação, de acordo com as boas práticas (APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança do COBIT 5.0);

g) implante sistema automatizado de gestão de acessos e autorizações aos sistemas i-Educar e Sigep, com validação periódica de cadastros por parte dos titulares das unidades administrativas, de forma que a gestão administrativa de pessoal opere de forma integrada e consistente com a gestão de acesso de sistemas pelos servidores da SEEDF;

III. autorizar o encaminhamento de cópias do Relatório Final de Auditoria, do Voto e da Decisão a ser proferida ao titular da SEEDF, para subsidiar a adoção das medidas e o retorno dos autos à Secretaria de Fiscalização Especializada para as devidas providências.

Brasília (DF), 31 de maio de 2019.

Marcelo Oliveira Vasconcelos
Auditor de Controle Externo

Everton Assumpção
Auditor de Controle Externo