TRIBUNAL DE CONTAS DO DISTRITO FEDERAL SECRETARIA DE FISCALIZAÇÃO ESPECIALIZADA DIVISÃO DE FISCALIZAÇÃO DE TECNOLOGIA DA INFORMAÇÃO	**Matriz de Achados**	Processo: 4093/2018

Objeto do Trabalho: 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.

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

QA 1: ? Os contratos que envolvem TIC são executados em conformidade com a legislação?

Ref	Achados de Auditoria	Critérios	Análises e Evidências	Causas	Efeitos	Proposições	Benefícios Esperados	Item
1.1	Descontinuidade dos serviços de enlace de comunicação de dados nas unidades educacionais	1.1.1 - Cumprimento das obrigações previstas em contrato, termo de referência/projeto básico e edital pelos fornecedores de bens e serviços. Lei 8.666/93 (artigos 66 ao 76) e IN nº 04/14 - SLTI/MPOG	A.1 - O Contrato nº 19/2013 , firmado entre a SEDF 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. Segundo informações do executor do contrato, encaminhadas por meio de despacho à Coordenação de Informática da SEEDF , 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 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. 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. 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 , considerando o desligamento dos serviços anteriormente fornecidos pela contratada, conforme se verifica no rack de parede com porta de vidro desativado. No entanto, restou evidenciado que a medida contingencialmente adotada pela SEDF não surtiu efeito, vez que das 31 escolas visitadas apenas duas noticiaram que utilizavam a verba do PDAF . Neste caso, constatou-se que a maioria 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. Para resolver a falta de acesso à Internet para operar os sistemas administrativos da SEEDF, observou-se que a maioria das escolas visitadas utilizam como forma de custeio desse serviço as Associações de Pais e Mestres - APM?s e/ou cotização entre os servidores. A situação atual demonstra a necessidade de a jurisdicionada retomar o fornecimento dos serviços de comunicação de dados e implantar solução global que atenda as unidades escolares, nos termos da IN SLTI/MPOG nº 04/2014, art.13 , inciso V, de forma a evitar as medidas contingenciais acima retratadas. Por meio de resposta à Nota de Auditoria nº 02-4093/2018 , a SEEDF noticiou novo processo licitatório para contratação de link de acesso à internet com previsão de publicação no primeiro semestre de 2018 , mas não finalizado até a conclusão deste relatório.	C.1 - Planejamento deficiente na alocação dos recursos financeiros que ensejou a suspensão dos serviços pela contratada por falta de pagamento. (A.1)	E.1 - Utilização precária dos sistemas de apoio escolar pelas unidades escolares. (A.1)	• Determinar à SE - Secretaria de Estado de Educação que: ◦ 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, (C.1; E.1; A.1;)	1. Garantir a disponibilidade de acesso à Internet para uso dos sistemas de apoio escolar.	1.1
1.2	Elevado índice de atendimento presencial, relativo a execução do Contrato nº 06/2016	1.1.2 - Fiscalização e controle da execução contratual pela Administração Pública e observância das exigências legais para processamento da liquidação da despesa (Lei 8.666/93, arts. 58, III. e 67); IN nº 04/14 - SLTI/MPOG; Decreto 32598/10, arts. 41,44 § único, 57 e 58 e Lei nº 4320/64, arts. 62 e 63. ITIL ? gestão de incidentes e COBIT DS8 - Gerenciar a Central de Serviço.	A.1 - 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. Os serviços prestados encontram-se categorizados por atividades e níveis para atendimento aos servidores das sedes/regionais de ensino da SEEDF e das unidades escolares, conforme recomendado pelas boas práticas de mercado (ITIL /COBIT). Ao examinar os relatórios de atividades, relativo ao período de abril/2016 a dezembro/2017 , 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. Da mesma forma, observa-se elevado atendimento de chamados presenciais, relativo ao período de janeiro de 2018 , 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, A situação acima evidenciada decorre de várias atividades/serviços escaladas para o nível de suporte presencial sem a devida necessidade , 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. 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 preconiza os frameworks de mercado (ITIL ? gestão de incidentes e COBIT DS8). 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).	C . 1 - 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. (A.1)	E . 1 - Deficiência na prestação do serviço realizado. Escalonamento do incidente, ocasionando dilatação do prazo (intempestividade) e custo da resolução do incidente. (A.1)	• Determinar à SE - Secretaria de Estado de Educação que: ◦ 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. (C.1; E.1; A.1;)	1. Melhoria na prestação de serviço realizado pelo Service Desk. Economia de recursos públicos.	1.1

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

Ref	Achados de Auditoria	Critérios	Análises e Evidências	Causas	Efeitos	Proposições	Benefícios Esperados	Item
2.1	Parque de computadores dos laboratórios de informática obsoleto.	2.1.1 - Meta/estratégia 7.12 ? Tecnologias educacionais do Programa Nacional de Educação ? PNE. ProInfo - Programa Nacional de Informática na Educação do MEC.	A.1 - 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. 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. Nesse sentido, visitou-se 31 escolas, representando 5% de cada Regional de Ensino do DF (extrato) 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. 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) , em razão da dificuldade de reposição de peças que necessitam de manutenção. 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. 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). 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. 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 . No entanto, quando o diagnóstico da equipe de manutenção se refere a peça danificada ou quebrada, não é possível repô-la, em razão de não ser mais fabricada. Assim, observa-se uma diminuição gradativa dos equipamentos 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) aos alunos no processo de ensino-aprendizagem.	C.1 - Carência de recursos financeiros para renovação do parque computacional instalado nos laboratórios de informática das escolas públicas do DF. (A.1)	E . 1 - Impossibilidade de utilizar o computador como ferramenta pedagógica. Ociosidade do laboratório de informática das escolas públicas por falta de equipamentos. (A.1)	• Recomendar à SE - Secretaria de Estado de Educação que: ◦ Recomendar à SEEDF que 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 visando a cessão de equipamentos. (C.1; E.1; A.1;)	1. Utilização plena do laboratório de informática. Estímulo ao aluno com o uso de novas tecnologias no processo ensino-aprendizagem.	2.1
2.2	Baixa velocidade do link de acesso à Internet disponibilizado nos laboratórios de informática das unidades escolares públicas do DF	2.1.2 - Meta/estratégia 7.12 ? Tecnologias educacionais do Programa Nacional de Educação ? PNE. Programa Banda Larga nas Escolas do FNDE.	A.1 - Conforme mencionado nos §§57/59 deste relatório, visitas ?in loco? foram realizadas com a finalidade de avaliar a oferta de TIC nas escolas públicas do DF para fins pedagógicos. Uma das tecnologias verificadas diz respeito à disponibilidade de link de acesso à internet nos laboratórios de informática. 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 das escolas preveem o uso de internet para atividades em classe, consoante estratégia (7.12) estabelecida pelo PNE. Na maioria das escolas visitadas (90%) verificou-se link de 1 (um) Mbps de velocidade média nos laboratórios de informática das unidades escolares Neste caso, o link disponibilizado pelo Programa Banda Larga nas Escolas - PBLE é compartilhado pelos alunos que se encontram conectados nos computadores da rede do laboratório de informática, conforme se observa na foto abaixo. Segundo informações dos diretores de escola, as aulas no laboratório de informática são realizadas com turmas de vinte alunos em média. Tomando como base esse parâmetro, disponibiliza-se por aluno somente 51,2 Kbps a ser consumido nas atividades de pesquisa/navegação de páginas/endereços pela internet. À título comparativo, conforme estudo publicado pela Ookla , 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). 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) em 2015. 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. 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. Com efeito, o aluno corre risco de não ter continuidade no seu aprendizado, pois a falta de conectividade impede a integração entre a pedagogia e o uso dos recursos digitais.	C.1 - Falta de recursos para ampliar a velocidade da Internet disponibilizada nos laboratórios de informática das escolas do DF. (A.1)	E . 1 - Impossibilidade de utilizar a internet como ferramenta pedagógica. (A.1)	• Recomendar à SE - Secretaria de Estado de Educação que: ◦ Recomendar à SEEDF que 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). (C.1; E.1; A.1;)	1. Uso de novas tecnologias no processo ensino-aprendizagem	2.1

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

Ref	Achados de Auditoria	Critérios	Análises e Evidências	Causas	Efeitos	Proposições	Benefícios Esperados	Item
			A.1 - 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. 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. O objetivo de um sistema de gestão de segurança da informação é preservação da confidencialidade, integridade e disponibilidade das informações. 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					

3.1	Baixo nível de maturidade de gestão de segurança da informação	3.1.1 - IN 04/2014-SLTI-MPOG e ABNT ISO/IEC 27002:13 (Capítulo 8). ABNT ISO/IEC 27004:2017. ABNT ISO/IEC 27005:2011. ABNT ISO/IEC 27014:2013. NIST SP 800-53A4 . Cobit 5.0 APO13 - Gerenciar Segurança, DSS04 - Gerenciar continuidade e DSS05 - Gerenciar serviços de segurança.	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. 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. No âmbito da Administração Pública do DF, existe um Centro de Processamento de Dados (Datacenter) na Secretaria de Planejamento (SEPLAG) que compartilha o uso de recursos computacionais com diversas outras secretarias de estado, dentre elas, a SEEDF. Os sistemas informatizados da SEEDF estão hospedados neste datacenter com algumas redundâncias de dados no centro de processamento de dados da Secretaria de Fazenda. As evidências constantes deste tópico estão presentes nas respostas 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). 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. A seguir, apresentam-se as análises por temática. Política e práticas de Segurança da Informação 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) (questão 107, nota nº 3);  política de avaliação de risco (inexiste) (questão 129, nota nº 3). O atual cenário da SEEDF é de quase inexistência de documentação que permita estabelecer as diretrizes de segurança de informação. 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. 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 das instituições. 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. O escopo da governança da segurança da informação abrange a 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. 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. 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. 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. 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. 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. 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 Identificação e acesso (Questões de 47 a 63 da Nota nº3) 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). 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 pelas ameaças, e pode causar danos aos ativos da organização, como alteração de informações, representando perda de confidencialidade e integridade dos sistemas. Gerenciamento de	C.1 - Inobservância das boas práticas dos processos de segurança da informação. (A.1)	E.1 - Melhoria da gestão de segurança da informação (A.1)	• Determinar à SE - Secretaria de Estado de Educação 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); (C.1; E.1; A.1;) ◦ 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.1; E.1; A.1;) ◦ Passe a adotar abordagem baseada em riscos para segurança da informação conforme estabelece a ISO 27.001, ISO 27.005 e ISO 27.014; (C.1; E.1; A.1;) ◦ 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). (C.1; E.1; A.1;) ◦ elabore e faça uso de termo que cientifique os usuários dos sistemas quanto a s suas responsabilidades e obrigações, bem como indicações de possíveis vulnerabilidades decorrentes do mal-uso dos sistemas, mantendo a guarda desses termos assinados pelos usuários; (C.1; E.1; A.1;) ◦ 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 (C.1; E.1; A.1;)	1. 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	3.1

			perda de confidencialidade e integridade dos sistemas Gerenciamento de riscos em Segurança da Informação (questões nos 129 a 132 da nota 3) Em resposta à nota de auditoria nº 3 , 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). 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. Os sistemas em exame (i-Educar e SiGEP) são acessados por meio da internet que se encontra em ambiente hostil , o que leva a alteração dos 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). 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. Maturidade do Processo de Segurança da Informação 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. 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. 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. Para identificar a 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.				
3.2	Capacidade insuficiente de a SEDF atender as demandas do Sistema i-Educar	3.2.1 - COBIT 5.0 BAI03.03 ? Desenvolver componentes da solução; BAI03.05 ? Construir soluções; BAI09 - Gerenciar ativos de TI.	A.1 - O Sistema i-Educar é um software de gestão escolar disponibilizado no Portal do Software Público Brasileiro , em 2008, por meio de um sistema com banco de dados centralizado e totalmente web. A principal finalidade do software é informatizar a gestão das informações educacionais, contribuindo com a racionalização do trabalho. No âmbito da SEDF, 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. 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 mercado (COBIT 5, BAI03.03, BAI03.03 e BAI09). 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. Em atendimento à Nota de Auditoria nº 04-4093/2018, a SEEDF disponibilizou relatório das demandas represadas (backlog) do sistema i-Educar, atualizado até o dia 15.05.18, considerando os tipos de serviços a serem executados. 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 essas demandas pela equipe atualmente alocada para manter o sistema, considerando que aproximadamente 51% das demandas (113), tem prioridade urgente, alta e imediata. Ainda, observa-se quantitativo expressivo de demandas para 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).	C.1 - Falta de priorização da gestão do projeto. Falta de pessoal especializado. (A.1)	E.1 - Potencial risco de não atender as demandas do sistema i-Educar. Não implementar melhorias capazes de otimizar a gestão escolar. (A.1)	• Recomendar à SE - Secretaria de Estado de Educação que: ◦ Recomendar à SEEDF que 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. (C.1; E.1; A.1;)	1. Diminuição do backlog atualmente existente do sistema i-Educar. Atendimento tempestivo das demandas.	3.2

Data de Elaboração: 11/07/2019 14:30:33 / Elaborado por: Everton Peixoto Correia de Assumpção (Coordenador), Marcelo Oliveira Vasconcelos / Supervisor: Flávio José Fonseca De Souza .