DILIGÊNCIA

Processo Nº:	TCE/009415/2016
Natureza:	Auditoria e Inspeção (Auditoria Operacional no Sistema Integrado de Material, Patrimônio e Serviços do Estado da Bahia - SIMPAS)
Vinculação / Unidade:	Secretaria da Administração (SAEB) / Superintendência de Recursos Logísticos (SRL)
Responsáveis:	Edelvino da Silva Góes Filho (Secretário)
	Jerusa Marins Paes Coelho (Superintendente da SRL)
Período:	Julho/2014 a dezembro//2015
Relator:	Cons. Pedro Lino
Exercícios:	2014 e 2015

Em atendimento ao despacho do Exmo. Sr. Conselheiro Relator (Ref.1854560-1), apresenta-se, na sequência, as conclusões da Auditoria após análise dos documentos e esclarecimentos carreados aos autos pelo Secretário da Administração do Estado da Bahia (Ref.1823744-1), Sr. Edelvino da Silva Góes Filho.

Cumpre informar que o Secretário, fundamentou sua resposta ao Ofício TCE nº 000225/2017/TCE/GAPRE/SEG nas justificativas apresentadas pela Superintendência de Gestão e Inovação – SGI (Ref.1823744-2 a 23) e pela Superintendência de Recursos Logísticos – SRL (Ref.1823744-26 a 43).

Importante frisar que a análise de tais esclarecimentos, em estrito cumprimento ao quanto determinado pelo Exmo. Sr. Cons. Relator, dirigiu-se especificamente à Promoção Ministerial (Ref. 1854445-3) que pugnou pela conversão do feito na presente diligência interna para:

> [...] que a Sexta Coordenadoria de Controle Externo proceda ao cotejamento entre os esclarecimentos prestados pelo gestor às fls. Ref.1823744-3/23 e as irregularidades identificadas pela 6ª CCE no Apêndice A de Ref. 1706289, indicando se as novas informações prestadas pelo gestor são capazes de modificar, em alguma medida, o Relatório de Auditoria inicial ou as recomendações inicialmente sugeridas.

Isto posto, a Sexta Coordenadoria de Controle Externo deste Tribunal e o Centro de Estudos e Desenvolvimento de Tecnologias para Auditoria (CEDASC), em consonância com o requisitado pela 4ª Procuradoria do Ministério Público de Contas do Estado da Bahia e tendo em vista o atendimento ao quanto determinado pelo Cons. Relator, em reexame dos autos, passam a apresentar, na sequência, as considerações que reputam ser dignas de destaque.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

DA ANÁLISE

ITEM 2.3 DEFICIÊNCIAS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO DO SIMPAS:

Item 2.3.1 Ausência de integridade entre as tabelas.

- *Promover avaliação completa acerca da ausência de implementação da integridade referencial nos bancos de dados dos sistemas SIMPAS e COMPRASNET.*

Em sua resposta a SAEB confirma que a integridade referencial nos bancos de dados pode ser implementada e que o esforço para tal estava em avaliação, portanto ainda não havia sido implementada até a ocasião do cotejamento entre os esclarecimentos prestados pelo gestor e as irregularidades identificadas pela auditoria.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Implementar integridade referencial entre as tabelas avaliadas como imprescindíveis.*

Em sua resposta a SAEB confirma que a integridade referencial nos bancos de dados pode ser implementada e que o esforço para tal estava em avaliação, portanto ainda não havia sido implementada até a realização dos trabalhos de cotejamento dos esclarecimentos do gestor e as irregularidades apontadas pela auditoria.

Opinião da auditoria: o achado de auditoria deve ser mantido.

Item 2.3.2 Operações realizadas sem a identificação do usuário responsável

- *Registrar na tabela de log a identificação completa e precisa do usuário que realizou acesso ao Sistema SIMPAS;*

Em sua resposta a SAEB informa que foi iniciado esforço para atender o item, portanto a funcionalidade ainda não havia sido atendida até a realização dessa diligência interna.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Implementar o recurso de integridade referencial entre as tabelas "Usuarios" do banco "SIMEB" e a tabela log, do banco "SIMESBAUDIT", de forma que só se permita a realização de operações no log com o devido reconhecimento do usuário na tabela do domínio "Usuarios";*

Em sua resposta a SAEB confirma que a integridade referencial solicitada pode ser implementada e que o esforço para tal estava em avaliação, portanto ainda não havia sido implementada até a realização da presente diligência interna.

Opinião da auditoria: O achado de auditoria deve ser mantido.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

- *Passar como parâmetro à Stored Procedure "up_resultado_dispensas_finalizada", o usuário conectado ao sistema, de forma a registrar no log o responsável pela operação*

Em sua resposta a SAEB informa que a *stored procedure* é realizada de forma automática, não existindo usuário responsável por sua execução, portanto não é possível registrar no *log* o responsável pela operação. Entretanto, é possível a SAEB implementar outra solução que assegure o registro do responsável pela operação.

Opinião da auditoria: O achado de auditoria deve ser mantido.

- *Manter registro do chamado que motivou a alteração, no caso de intervenções diretas no banco de dados.*

A evidência apresentada pela SAEB de que há registros no sistema *RedMine* de chamados motivando intervenção direta no banco de dados é de fevereiro de 2017, período fora do escopo da auditoria que foi de janeiro a dezembro de 2015. Assim não é possível afirmar que a SAEB possuía tal controle à época da realização dos procedimentos.

Opinião da auditoria: o achado de auditoria deve ser mantido.

Item 2.3.3 Operações realizadas por usuários sem permissão de acesso

- *Criar norma que discipline os usuários, seus vínculos, cargos e funções aptos a executar as operações no sistema SIMPAS, seguida da sua devida institucionalização e divulgação aos usuários do sistema e responsáveis em cadastrar as permissões de acesso;*

- *Revisar os dados da tabela "Funcoes_usuarios" padronizando o registro das informações e corrigindo as falhas;*

Em sua resposta a SAEB informa que foi iniciado esforço para atender a recomendação, portanto a funcionalidade ainda não havia sido atendida até a realização desta diligência interna.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Implementar exclusão lógica dos registros da tabela "Funcoes_usuarios" na operação "Delegar Direitos", citada na justificativa da SAEB. A exclusão física dos registros, como feita atualmente, apaga a evidência que as permissões de acesso foram concedidas corretamente no momento da realização da operação;*

Em sua resposta a SAEB informa que foi iniciado esforço para atender sem, entretanto, fixar prazo para a implementação da recomendação, portanto a funcionalidade ainda não havia sido atendida até a realização dessa diligência.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Alterar a estrutura da tabela "Funcoes_usuarios" de forma a associar as permissões de acesso aos módulos e operações do sistema, a perfis de grupos de usuários, em vez de associá-los diretamente ao usuário, como atualmente implementado. Dessa forma, o*

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

gerenciamento do cadastro das permissões de acesso ao SIMPAS ficará mais simples, tornando possível a aderência a norma que disciplina os acessos;

Em sua resposta a SAEB apresenta argumentos para não implementar a orientação, mas que cabe a área de negócio avaliar os impactos da mudança proposta. Entretanto, não identificou-se nenhuma informação da área de negócio sobre a recomendação da auditoria. Portanto, a funcionalidade solicitada ainda não existe no sistema.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Mapear os acessos indiretos às operações do sistema, realizando a devida correspondência destes acessos a tabela de permissões. Não se deve permitir, por exemplo, que uma operação de atualização na tabela "req_mat_serv", feita pelo modulo de Licitação, seja concedida sem que este usuário realizando a operação na Licitação também tenha permissão ativa ao modulo de Requisição de Material e Serviço.*

A SAEB informou que executa o controle de permissões de acesso às funcionalidades através da rotina de Direitos Delegados, garantindo que uma operação de atualização na tabela *red_mat_serv* só seja feita por um usuário que tenha permissão de execução dessa funcionalidade, entretanto não apresentou evidências sobre a execução desse procedimento.

Opinião da auditoria: o achado de auditoria deve ser mantido.

Na sequência, serão analisados os esclarecimentos e documentos apresentados pela SAEB acerca dos pontos relacionados pela auditoria no Anexo A (Ref. 1706289 e 1823744-6/23).

ITEM 03 - GERENCIAMENTO DE RECURSOS HUMANOS E ITEM 08 - GERENCIAMENTO DE TERCEIRIZAÇÃO

A respeito das fragilidades relacionadas com o Gerenciamento de Recursos Humanos, a SAEB alegou que:

> Não procede o questionamento do TCE em relação a Gestão de Recursos Humanos, uma vez que o Serviço ofertado pela PRODEB compreende na Prestação de serviços técnicos de informática para sustentação dos Sistemas Corporativos do Estado da Bahia, aqui relacionado o SIMPAS/COMPRASNET, no que diz respeito à sua manutenção corretiva e adaptativa, de acordo com as condições oferecidas na proposta de serviços 233/2010 que deu origem ao contrato 001.11.27.CN.0. Desta forma não há oferta de Recursos Humanos, e sim de serviços técnicos com escopo e níveis de serviços definidos. Outrossim, a responsabilidade pela gestão dos recursos humanos utilizados na prestação do referido serviço é de inteira responsabilidade da PRODEB, que como Empresa prestadora de serviços de TI deve observar o fiel cumprimento da Legislação trabalhista e previdenciária.

O fato do serviço ofertado pela PRODEB compreender a prestação de serviços técnicos de informática para sustentação dos sistemas e não a oferta de recursos humanos, já havia sido observado pela auditoria, mas essa condição não exime a necessidade da administração fiscalizar o bom gerenciamento dos recursos humanos que atuam na prestação do serviço sem prejuízo da verificação do cumprimento da legislação trabalhista e previdenciária.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

No contexto do serviço em foco, o gerenciamento dos recursos humanos poderia ser realizado pela PRODEB, mas a auditoria já havia registrado em seu relatório que a PRODEB informou não existir responsabilidades formalizadas em relação ao referido gerenciamento. Portanto, os esclarecimentos apresentados pela SAEB não alteraram o entendimento inicial da auditoria em relação ao Gerenciamento de Recursos Humanos relacionados aos serviços dos sistemas SIMPAS/COMPRASNET.

Destacamos que a SAEB apresentou relatório assinado pela empresa certificadora IMPLEMENTUM atestando que a Gerência de Soluções 1 da PRODEB foi avaliada e satisfez os requisitos dos processos Gerência de Projetos e Gerência de Requisitos, sendo classificada como aderente ao Nível G da versão 2016 do Modelo de referência MR-MPS-SW, que visa a Melhoria de Processo de Software e Serviços.

No Item 07 – Observações Gerais Quanto ao Modelo, deste relatório, é destacado que a implementação dos processos de Garantia da Qualidade e Gerência de Recursos Humanos é um ponto forte da metodologia utilizada pela PRODEB. Entretanto, não foram apresentadas evidências de que o gerenciamento de recursos humanos tenha sido aplicado na prestação dos serviços para manutenção corretiva e adaptativa do SIMPAS/COMPRASNET. Importante frisar que esse relatório também é de 2016, sendo posterior à realização da auditoria.

Opinião da auditoria: o achado de auditoria deve ser mantido.

ITEM 04 - AVALIAÇÃO E GERENCIAMENTO DE RISCOS

A seguir serão analisados os esclarecimentos e documentos apresentados pela SAEB a respeito das fragilidades apontadas pela auditoria, relacionadas ao tema Avaliação e Gerenciamento de Riscos.

FRAGILIDADES IDENTIFICADAS:

1. **Resposta da SAEB ao check list de processos, atividades, padrões, boas práticas e controles de TI, seção "AVALIAÇÃO E GERENCIAMENTO DE RISCOS", que apontam a inexistência dos seguintes controles:**

   - ***Análise de riscos relacionados a TI;***

   A SAEB informa que, apesar da falta de contrato de suporte, é possível realizar análise de risco com a ferramenta *Risk Manager*, mas não informa se a análise foi realizada nem apresenta nenhuma evidência de sua realização.

   Opinião da auditoria: o achado de auditoria deve ser mantido.

   - ***Uso de sistema informatizado para gerenciamento de riscos;***

   A SAEB limitou-se a informar que o gerenciamento de riscos depende de investimento na renovação do contrato de suporte do *Risk Manager* e em contratação do serviço junto à PRODEB.

   Opinião da auditoria: o achado de auditoria deve ser mantido.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

- *Participação de TI em grupos especializados em gerenciamento de riscos para troca de experiências.*

A SAEB informou que a equipe de Segurança da Informação (SI), bem como equipes da PRODEB participam de fóruns relacionados com o tema, mas não apresentou evidências de participação da equipe em tais grupos ou eventos temáticos.

Opinião da auditoria: o achado de auditoria deve ser mantido.

2. Resposta da SAEB ao check list de processos, atividades, padrões, boas práticas e controles de TI, seção "AVALIAÇÃO E GERENCIAMENTO DE RISCOS", que apontam os itens abaixo como não existentes para o SIMPAS e Comprasnet.ba, mas já sendo contemplados no processo de desenvolvimento atual, podendo ser aplicados a evoluções do sistema, porém sem evidências de comprovação:

- *Ações de mitigação de riscos;*

Quadro 01 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
04 - Ferramenta análise de vulnerabilidade - Acunetix;	*Printscreen* de tela do sistema.	Não demonstra o que o sistema faz nem que ele foi utilizado na gestão de riscos do SIMPAS/COMPRASNET
04 - Ferramenta análise de vulnerabilidade - Arachni.		

Os documentos encaminhados pela SAEB apenas apresentam telas das ferramentas Acunetix e Arachni, que não evidenciam que as mesmas foram utilizadas na prestação dos serviços prestados à SAEB.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- Programa de capacitação em gerenciamento de riscos;

Quadro 02 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
04 - Auditor interno ISO 20000	Certificado de treinamento do técnico da PRODEB em curso na área de segurança.	A disciplina de segurança da informação abrange tópicos de gestão de riscos.
04 - Certificacao Universal - ISO 27002		
04 - Certificado EXIN oficial ISO-27002		
04 - Certificado_Encontro_GTSI		
04 - MTA - Security Fundamentals		
04 - MTA - Security Fundamentals		
04 - Security Officer 1		
04 - Security Officer 2		
04 - Risk Manager	Certificado de treinamento do técnico da PRODEB em curso na área de gestão de riscos em 2010.	Evidência de um curso na área de gestão de riscos.

Os certificados apresentados, com exceção do “04 – Risk Manager”, comprovam que técnicos da PRODEB participaram de treinamentos relacionados com a disciplina de segurança da informação. Apesar da análise de risco ser uma das disciplinas abordadas pela segurança da informação, uma não se confunde com a outra, portanto os certificados apresentados não garantem que os técnicos da PRODEB participaram de capacitação com conteúdo de

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

gerenciamento de riscos e dominam as ferramentas necessárias para a realização da Gestão de Riscos e principalmente não asseguram que essas técnicas e ferramentas foram aplicadas na prestação dos serviços prestados à SAEB.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Identificação dos riscos de maior impacto ao negócio;*

A SAEB limitou-se a informar que a PRODEB possui um processo de identificação de riscos tecnológicos e reconhece que seus impactos não são vinculados ao negócio. Se a SAEB realizasse esse procedimento bastaria apresentar a lista dos riscos de maior impacto ao negócio, identificados no período.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Revisão periódica nos riscos de TI em função de alterações no negócio ou no ambiente de TI;*

A SAEB limitou-se a informar que a PRODEB possui um processo de identificação de riscos tecnológicos, e seus impactos não são vinculados ao negócio.

Opinião da auditoria: o achado de auditoria deve ser mantido.

RECOMENDAÇÕES DA AUDITORIA:

1. **Treinar os técnicos e usuários em análise de riscos e envolvê-los no processo de gerenciamento de risco;**

   Nos esclarecimentos apresentados pelos gestores, a SAEB confirma a necessidade de treinamentos, o que ratifica a permanência da recomendação.

2. **Utilizar uma ferramenta automatizada para o gerenciamento de riscos;**

   A SAEB limitou-se a dizer que a utilização da ferramenta automatizada *Risk Manager* depende de investimentos. Os argumentos apresentados não elidem a pertinência dessa recomendação.

3. **Participar de grupos especializados em gerenciamento de riscos para troca de experiências;**

   A SAEB informou, sem apresentar evidências, que a equipe de Segurança da Informação e a PRODEB participam de fóruns e grupos relacionados com a segurança da informação. Não identificamos, entretanto, argumentos aptos a afastar a recomendação.

4. **Utilizar a norma brasileira NBR ISO 27002, que trata das boas práticas na gestão da segurança da informação, como guia para padronização nos processos de gestão do risco na instituição.**

   A SAEB informou que a PRODEB segue a norma NBR ISO 27002, que trata de boas práticas para gestão da segurança da informação, e apresentou evidências da certificação de dois

Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3
Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.

técnicos em *Information Security Foundation,* curso cujo conteúdo é baseado na norma brasileira ISO/IEC 27002. Desta forma, considerando o fato da PRODEB já trabalhar com a referida norma, reforça-se a recomendação para que aproveite o conhecimento já internalizado para a padronização dos processos de gestão de risco na instituição.

ITEM 05 - DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

A SAEB não apresentou esclarecimentos e documentos sobre as fragilidades identificadas pela auditoria para o tópico desenvolvimento e manutenção de sistemas, ao invés disso encaminhou considerações sobre as recomendações apresentadas. Ressaltamos que as recomendações são estratégias sugeridas pelo TCE, com base nas disciplinas do COBIT, para mitigar as fragilidades encontradas e que a resolução dessas fragilidades é obtida com a execução do conjunto das estratégias, portanto concluímos que o material apresentado não enseja a modificação nas fragilidades identificadas pela auditoria.

A seguir serão analisados os esclarecimentos e documentos apresentados para cada recomendação.

1. Formalizar metodologia para o processo de desenvolvimento de sistemas.

Quadro 03 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
05 – Relatório final de Avaliação MPS.BR Nivel G (emitido pela IMPLEMENTUM)	Relatório de avaliação da aderência do processo de software da PRODEB ao modelo de referência de processo MR-MPS-SW versão 2016, para o nível G.	Evidência de existência formal de uma metodologia de desenvolvimento de sistema em 2016.
05 – Processo de Desenvolvimento Tradicional	Documento que descreve as etapas e atividades do processo de desenvolvimento de sistemas da PRODEB.	Evidência de existência formal de uma metodologia tradicional de desenvolvimento de sistema.
05 – Processo de Desenvolvimento Ágil	Documento que apresenta as principais atividades que devem ser realizadas durante a execução de um projeto utilizando métodos ágeis.	Evidência de existência formal de uma metodologia ágil de desenvolvimento de sistema.
05 – *Template* – Checklist de Auditoria de Qualidade Tradicional	*Template* de *checklist* de auditoria de qualidade de conformidade em processos, procedimentos e orientações para desenvolvimento de projeto de software.	Evidência de existência formal de uma metodologia tradicional de desenvolvimento de sistema.
05 – *Template* – Checklist de Auditoria de Qualidade - Ágil	*Template* de *checklist* de auditoria de qualidade para desenvolvimento de projeto ágil.	Evidência de existência formal de uma metodologia ágil de desenvolvimento de sistema.

As evidências encaminhadas pela SAEB confirmam a existência de metodologia para o processo de desenvolvimento de sistemas na PRODEB.

Opinião da auditoria: a recomendação da auditoria deve ser suprimida uma vez que a PRODEB já possui metodologia formalizada para o processo de desenvolvimento de sistemas.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

2. Alinhar o processo de desenvolvimento de sistemas com a estratégia de negócio contemplando todos os projetos.

Quadro 04 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
05 – *Template* – Documento de Visão do Negócio	*Template* de documento de Visão do Negócio	Evidência de que há previsão de levantamento de informações relacionadas ao negócio na fase inicial de novos projetos.
05 – *Template* – Estratégia de Implementação Preliminar	*Template* de documento de Implementação Preliminar	Evidência de que há previsão de levantamento de aspectos importantes relativos ao negócio na fase de planejamento de novos projetos.
05 – *Template* – Termo de Homologação do Produto	*Template* de Termo de Homologação do Produto	Evidência de que o gestor do negócio é envolvido na fase de entrega de produtos.

Os documentos apresentados pela SAEB evidenciam que na metodologia de desenvolvimento de sistema da PRODEB há processos para o levantamento de informações relacionadas ao negócio em novos projetos que permitem o alinhamento do processo de desenvolvimento de sistemas com a estratégia de negócio, mas, como já havia sido apontado no relatório de auditoria (Ref. 1706289-22), esse procedimento não é aplicado em casos de manutenção como o prestado para o SIMPAS/COMPRASNET.

Se o alinhamento entre o processo de desenvolvimento com a estratégia de negócio estivesse sendo aplicada ao processo de manutenção, bastaria a SAEB ter encaminhado os *templates* apresentados no caso do SIMPAS/COMPRASNET.

Opinião da auditoria: a recomendação deve ser mantida.

3. Aplicar a metodologia de desenvolvimento e manutenção de sistemas em toda a organização e seus projetos;

4. Formalizar a melhoria contínua da metodologia de manutenção de sistemas que hoje ocorre de forma empírica;

5. Utilizar referência bibliográfica para a metodologia de manutenção de sistemas;

6. Criar modelos pré-definidos de documentos a serem utilizados na metodologia de manutenção de sistemas.

A resposta a seguir trata das recomendações 3, 4, 5 e 6, supramencionadas.

Quadro 05 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
05 – Modelo Gestão do Relacionamento SAEB	Descrição dos processos para gestão do relacionamento entre a Companhia de Processamento de Dados do Estado da Bahia – PRODEB, e a Secretaria de Administração do Estado da Bahia – SAEB.	Evidência de processo de gestão do relacionamento
05 – Orientações_para_Utilizacao do_Redmine	Apresenta instruções de como cadastrar os *tickets* na ferramenta *Redmine*, visando gerar uma padronização que oriente os usuários do sistema.	Evidência de processo formal para abertura e registro de demandas de manutenção.

As evidências apresentadas pela SAEB demonstram que existe um processo formalizado na PRODEB que orienta o relacionamento entre esta e os seus clientes no processo de gestão do relacionamento e na abertura e gestão das demandas em contratos de manutenção, entretanto as evidências apresentadas não são suficientes para atender às recomendações.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

O modelo de gestão de relacionamento e a ferramenta automatizada para gestão de demandas (*Redmine*) é apenas uma parte da metodologia de desenvolvimento e manutenção de sistemas, foco das recomendações 3, 4, 5 e 6, apresentadas pela auditoria.

Opinião da auditoria: as recomendações devem ser mantidas.

ITEM 07 - GERENCIAMENTO DE MUDANÇAS

A SAEB não apresentou esclarecimentos e documentos para as fragilidades identificadas pela auditoria para o tópico gerenciamento de mudanças, ao invés disso encaminhou considerações sobre as recomendações apresentadas. Ressaltamos que as recomendações são estratégias sugeridas pelo TCE, com base nas disciplinas do COBIT, para mitigar as fragilidades encontradas e que a resolução dessas fragilidades é obtida com a execução do conjunto das estratégias, portanto indicamos que o material apresentado não enseja a modificação nas fragilidades identificadas.

A seguir serão analisados os esclarecimentos e documentos apresentados para cada recomendação.

1. Realizar capacitação da equipe para implantação de um projeto específico de gerenciamento de mudanças;

Quadro 06 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
07 – Gerenciamento de Mudanças Manual do Processo R16.	Manual do processo de gerenciamento de mudanças.	Evidência da existência de um processo formal para gerenciamento de mudanças, mas não da sua aplicação efetiva.

O relatório de auditoria já havia identificado que:

> A SAEB informou que existe processo estabelecido de gerenciamento de mudanças desde 2005, (...)
>
> A SAEB informou que existem responsáveis definidos pela realização do gerenciamento de mudanças também desde 2005, indicando como evidência o sistema Redmine e não uma unidade administrativa em si.
>
> Não é realizado controle de atualização da documentação em função das mudanças.
>
> Foi informado que é realizada análise de impacto das mudanças sobre o negócio desde 2005. Para esta atividade, foi indicado como evidência o levantamento de requisitos, documento que de fato não comprova a prática.
>
> A SAEB respondeu que as mudanças podem ser identificadas através de registros desde 2005 e forneceu como evidência, novamente, uma tela do sistema Redmine. Porém, informou que a documentação de configuração necessária à realização da mudança não está atualizada.
>
> Não é utilizada ferramenta para detecção de software não autorizado ou não licenciado. (...)
>
> (...) as evidências fornecidas não indicam existir registro de erros ou de interrupções no ambiente de produção. As evidências também não esclarecem como é realizado o monitoramento da qualidade e desempenho do processo de

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

gerenciamento de mudanças, nem que existe reavaliação contínua do processo, através a (sic) avaliação do resultado desse monitoramento. Além disso não fica evidenciado se são definidos responsáveis pela realização do gerenciamento de mudanças, apenas que existem responsáveis designados por realizar mudanças quando um chamado é aberto.

Opinião da auditoria: os documentos apresentados não alteram o entendimento inicial da auditoria, assim sendo, resta mantida a recomendação.

2. Contemplar no projeto processo específico de registro e investigação de incidentes e fragilidades.

Quadro 07 – Análise dos documentos apresentados pelos gestores da SAEB.

Documento	Do que se trata	Avaliação
07 - RMD concluída com problema	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de requisição de mudança (RMD).	Evidência do processo de ordem de serviço a partir de uma requisição de mudança (RMD). Evidência que houve registro de problemas na execução de ordem de serviço da UNEB.
07 - RMD SIMPAS	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de requisição de mudança (RMD).	Evidência de serviço do SIMPAS realizado por meio do Sistema Integrado de Gestão de TI.
07 – Ata_comite_2016701	10 – Ata_comite_20160701	Evidência da realização de reunião do Comitê de Qualidade para tratar das Requisições de Mudanças (RMD) em aberto.

Os documentos apresentados evidenciam a existência de um processo de gerenciamento de mudanças, contemplando a avaliação de impacto no atendimento de solicitações dos clientes, bem como o registro de erros e problemas na execução dessas solicitações, mas não evidencia a existência de um processo específico para investigação de incidentes e fragilidades conforme indicado pela recomendação.

Opinião da auditoria: manter a recomendação.

3. Controlar a atualização da documentação dos ativos em função das mudanças.

Quadro 08 – Análise dos documentos apresentados pelos gestores da SAEB]

Documento	Do que se trata	Avaliação
07 - RMD concluída com problema	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de requisição de mudança (RMD).	Evidência do processo de ordem de serviço a partir de uma requisição de mudança (RMD). Evidência que houve registro de problemas na execução de ordem de serviço da UNEB.
07 - RMD SIMPAS	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de requisição de mudança (RMD).	Evidência de serviço do SIMPAS realizado por meio do Sistema Integrado de Gestão de TI.
07 – SIGSTI	Tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de ativos de TI da SAEB
07 – SIGSTI – Inventário de Componentes	Tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de ativos de TI da SAEB
07 – IC SIMPAS no CMDB	Tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de itens de configuração (IC) da SAEB

As evidências apresentadas confirmam que a PRODEB mantém um sistema para gestão de ativos que permite a identificação da configuração dos ambientes e ativos relacionados aos serviços prestados, entretanto não suficientes para comprovar que esse sistema permite

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

recuperar o momento em que uma mudança foi realizada nem a configuração de um ambiente em uma data específica no passado.

Opinião da auditoria: manter a recomendação.

4. Manter atualizada a documentação de configuração necessária a realização da mudança.

Quadro 09 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
07 – SIGSTI	*Printscreen* de tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de ativos de TI da SAEB
07 – SIGSTI – Inventário de Componentes	*Printscreen* de tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de ativos de TI da SAEB
07 – IC SIMPAS no CMDB	Tela do Sistema Integrado de Gestão de Serviços de TI	Evidência da utilização de ferramenta para gestão de itens de configuração (IC) da SAEB

Foram apresentados os documentos descritos na Quadro 9. A SAEB informou que com o apoio do processo de configuração, ficam registradas também no CMDB as novas características do IC (item de configuração) e quando o mesmo foi alterado. Contudo, não é possível afirmar pela análise das evidências apresentadas que a documentação é mantida atualizada.

Opinião da auditoria: manter a recomendação.

5. Adotar ferramenta para a gestão de mudanças, tais como controle de versão e registro de atualização de versões do SIMPAS.

Quadro 10 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
07 – Redmine – COMPRAS-NET – PLANEJAMENTO	*Printscreen* de tela do Sistema Redmine	Evidência de conjunto de correções no COMPRASNET agrupada.
07 – Redmine – SIMPAS – PLANEJAMENTO	*Printscreen* de tela do Sistema Redmine	Evidência de conjunto de correções no SIMPAS agrupada.

Foram fornecidos documentos relativos a duas telas do sistema *Redmine*, indicando que foram abertos chamados para realização de tarefas no Sistema SIMPAS e no ComprasNet, mas não comprovam que está sendo usada ferramenta para controle de versões e registro de atualização de versões do SIMPAS.

Opinião da auditoria: manter a recomendação.

6. Utilizar ferramenta para detecção de software não autorizado ou não licenciado.

A SAEB informou que a PRODEB utiliza ferramenta de inventário de hardware e software, mas não informou se esta realiza detecção de software não autorizado ou não licenciado, nem apresentou evidências.

Opinião da auditoria: manter a recomendação.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

ITEM 10 - SEGURANÇA DE SISTEMAS

Para esse tópico, a SAEB apresentou esclarecimentos e documentos tanto para as fragilidades identificadas como para as recomendações sugeridas pela auditoria:

FRAGILIDADES

1. Resposta da SAEB ao check list de processos, atividades, padrões, boas práticas e controles de TI, seção "SEGURANÇA DE SISTEMAS", que apontam a inexistência dos seguintes controles:

- *Monitoramento e avaliação da eficiência da política de segurança:*

Para a fragilidade relacionada ao monitoramento e avaliação da eficiência da política de segurança, a SAEB apresentou documentos relacionados com as áreas de Gestão de Incidentes e Gestão de Mudanças.

Quadro 11 – Análise dos documentos apresentados pelos gestores da SAEB

Evidências Gestão de Incidentes		
Documento	**Do que se trata**	**Avaliação**
10 – Gestão de Incidentes Colaboradores	Apresentação tipo *PowerPoint* sobre o processo de Gestão de Incidentes na PRODEB.	Evidência da existência de um processo formal para gestão de incidentes, mas não da sua aplicação efetiva.
10-Gestão de Serviços de TI – Relatório de Estatísticas JULHO 2016	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de gestão de incidentes e problemas para os serviços hospedados no DataCenter da PRODEB.
10 – Modelo de Gestão de Incidentes – Redesenho de Processos	Descrição do processo de Gerenciamento de Incidentes da PRODEB. Documento elaborado pela empresa Allen, contratada da PRODEB.	Outra evidência da existência de um processo formal para gestão de incidentes, mas não da sua aplicação. Não foi possível confirmar a compatibilidade com o fluxo do documento *10 – Gestão de Incidentes Colaboradores*.
10 – Notificação de Incidentes de vulnerabilidade de Segurança em Sites e Aplicações Web – Estrutura de Processos	Descrição do processo de notificação de incidentes e vulnerabilidades de segurança em sites e aplicações Web.	Evidência da existência de um processo formal para notificação de incidentes e vulnerabilidades de segurança em sites e aplicações web, mas não da sua aplicação efetiva.
10 – Gerência de Incidentes_Manual de Processos_R2	Manual de Processo de Gerenciamento de Incidentes.	Evidência da existência de um processo formal para gestão de incidentes, mas não da sua aplicação efetiva. Não foi possível confirmar a compatibilidade com os outros 2 fluxos apresentados anteriormente.
10 – Gestão dos Serviços de TI – Relatório de Estatísticas Bimestral Julho-Agosto	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de gestão de incidentes e problemas para os serviços hospedados no DataCenter da PRODEB.
10 – Dica – ITIL2	Diagrama com orientação relacionada com o processo de gestão de incidentes.	Evidência de iniciativa relativa a capacitação dos técnicos na aplicação do processo de gestão de incidentes.
10 – Incidentes – Classificação Disponibilidade	Gráfico com a quantidade de incidentes conforme classificação de disponibilidade.	Evidencia de que há o registro e acompanhamento do quantitativo de incidentes.
10 – Modelo de Gestão de Incidentes críticos V2.3	Fluxograma.	O documento está ilegível.

Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3
Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.

Quadro 12 – Análise dos documentos apresentados pelos gestores da SAEB

Evidências Gestão de Mudanças		
Documento	**Do que se trata**	**Avaliação**
10 – Ata_comite_20160701	Ata da reunião do Comitê de Qualidade que discutiu o processo de tratamento das Requisições de Mudanças (RMD).	Evidência da realização do processo de gestão de mudanças. Obs: Mudança é tratada como qualquer solicitação de realização de serviço.
10 – Gerenciamento de Mudanças_Manual do Processo_R16	Manual do processo de gerenciamento de mudanças.	Evidência da existência de um processo formal para gerenciamento de mudanças, mas não da sua aplicação efetiva.
10 – Gestão de Serviços de TI – Relatório de Estatísticas JULHO 2016	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de gestão de incidentes e problemas para os serviços hospedados no DataCenter da PRODEB.
10 – Gestão de Serviços de TI – Relatório de Estatísticas Bimestral Julho-Agosto	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de gestão de incidentes e problemas para os serviços hospedados no DataCenter da PRODEB.
10 - RMD concluída com problema	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de RMD.	Evidência do processo de ordem de serviço a partir de uma RMD. Evidência de que os problemas na execução das ordens de serviço são registrados.
10 - RMD SIMPAS	Extrato de RMD/Atividade por Técnico. Registro da realização de ordens de serviço decorrentes de RMD.	Evidência de serviço do SIMPAS realizado por meio do Sistema Integrado de Gestão de TI.
10 - Dica – ITIL1	Diagrama com orientação relacionada com o processo de gestão de mudanças.	Evidência de iniciativa relativa a capacitação dos técnicos na aplicação do processo de gestão de mudanças.
10 – COMUNICADO – Alteração no processo de Gestão de Mudança	Comunicado sobre alteração do processo de Gestão de Mudança.	Evidência de que alterações no processo de Gestão de Mudança são comunicadas para a empresa.
10 – Gestão de Mudança Colaboradores 2014	Apresentação tipo PowerPoint sobre o processo de Gestão de Mudanças na PRODEB.	Evidência da existência de um processo formal para gestão de mudanças, mas não da sua aplicação efetiva.

Os diversos documentos apresentados demonstram em sua maioria a existência de norma formal na PRODEB para a gestão de incidentes e gestão de mudanças, situação que já havia sido identificada pela auditoria anteriormente:

> Existem diversos documentos que orientam ou dão embasamento à política de segurança da informação na PRODEB. Foi apresentado como evidência, entre outros documentos, as "Normas de Segurança da Informação", versão 3.0, de novembro de 2015, do Governo do Estado da Bahia, que se aplica a entidades da Administração Pública do Poder Executivo Estadual, com o objetivo de auxiliar na Gestão da Segurança da Informação. O documento é composto de 17 normas que compostas de sessões de objetivos, definições, abrangência, diretrizes, competências, etc. Referente à PRODEB, de forma específica, foi apresentada a resolução RD. 2001.001, de 13/08/2007, que institui o Comitê de Segurança Integrada, que tem por finalidade manter atualizada a Política de Segurança da PRODEB e realizar outras atividades relacionadas a segurança. Foram apresentados documentos referentes a normas permanentes da PRODEB que regulamentam uso de dispositivos móveis, proteção contra código malicioso,

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

backup/restore de dados do Data Center, uso de ferramentas de colaboração, controle de acesso ao Data Center da PRODEB e uso da internet e mídias sociais.

Entretanto, já haviam sido identificados como documentos de orientação para a realização da atividade/controle, mas que não comprovam que a atividade de orientação está sendo realizada.

A SAEB, para a fragilidade de *Monitoramento e avaliação da eficiência da política de segurança,* apresentou evidências relacionadas com os processos de gestão de mudanças e gestão de incidentes, contudo, não forneceu evidências do funcionamento do Comitê de Segurança Integrada que deveria avaliar periodicamente se a política de segurança adotada pela empresa está sendo empregada, se está gerando os resultados esperados e se seriam necessários ajustes e alterações nessa política.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Classificação de respostas por tipo de vulnerabilidade de segurança.*

Quadro 13 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
10 – Gestão de Mudança Colaboradores 2014	Apresentação tipo *PowerPoint* sobre o processo de Gestão de Mudanças na PRODEB.	Apresenta classificação e abrangência para mudanças, mas não para resposta por tipo de vulnerabilidades de segurança.
10 – Dica – ITIL2	Diagrama com orientação relacionada com o processo de gestão de incidentes.	Não trata da classificação de resposta por tipo de vulnerabilidade de segurança.
10-Gestão de Serviços de TI – Relatório de Estatísticas JULHO 2016	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de análise de vulnerabilidades para hospedagem de sites.
10 – Incidentes – Classificação Disponibilidade	Gráfico com a quantidade de incidentes conforme classificação de disponibilidade	Classifica apenas a indisponibilidade em parcial ou total.
10 – Modelo de Gestão de Incidentes – Redesenho do Processos	Descrição do processo de Gerenciamento de Incidentes da PRODEB. Documento elaborado pela empresa Allen, contratada da PRODEB.	Outra evidência da existência de um processo formal para gestão de incidentes, mas não para resposta por tipo de vulnerabilidades de segurança.
10 – Modelo de Gestão de Incidentes críticos V2.3	Fluxograma	O documento está ilegível.
10 – Notificação de Incidentes e Vulnerabilidade de Segurança em Sites e Aplicações Web – Estrutura do Processo V2	Descrição do processo de notificação e tratamento de incidentes e vulnerabilidades de segurança em sites e aplicações Web.	Evidência da formalização de processo para tratamento de vulnerabilidade de segurança em sites e aplicações Web. O documento não trata da classificação da resposta.
10 – Gerencia de Incidentes_Manual de Processos_R2	Manual de Processo de Gerenciamento de Incidentes.	Evidência da existência de um processo formal para gestão de incidentes, mas não para resposta por tipo de vulnerabilidades de segurança.
10 – Gestão de Serviços de TI – Relatório de Estatísticas Bimestral Julho-Agosto	Relatório apresentando estatísticas relacionadas aos processos de Gerenciamento de Mudanças, Incidentes, Problemas, Configuração, Capacidade, Requisição de Serviços e Segurança dos serviços hospedados no Datacenter PRODEB.	Evidência da aplicação do processo de análise de vulnerabilidades para hospedagem de sites.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

Os documentos apresentados não alteram o entendimento inicial da auditoria, conforme trecho transcrito a seguir:

> Para evidenciar que é realizado monitoramento de vulnerabilidades, ameaças e incidentes foram apresentados documentos referentes aos processos de "Análise de Vulnerabilidades em Código-fonte de Sites e Aplicações Web" e de "Notificação de Incidentes e Vulnerabilidades de Segurança em Sites e Aplicações Web". A sessão "Objetivo" desses documentos explica que a finalidades destes e apresentar a estrutura desses processos. São documentos de orientação para realização da atividade/controle, mas que não comprovam que a atividade está sendo realizada

Opinião da auditoria: o ponto deve ser mantido.

2. Respostas da SAEB ao check list de processos, atividades, padrões, boas práticas e controles deli, seção "SEGURANÇA DE SISTEMAS", que afirmam que os seguintes controles existem, porém não foram fornecidas evidências ou as evidências fornecidas não comprovam a existência do controle:

- *Avaliação periódica de privilégios de acesso*

A resposta da SAEB está tarjada no documento, não sendo possível cotejar os esclarecimentos dos gestores sobre as irregularidades apontadas no relatório de auditoria.

Opinião da auditoria: o achado deve ser mantido.

- *Segurança de rede – segmentação*

Quadro 14 – Análise dos documentos apresentados pela SAEB

Documento	Do que se trata	Avaliação
10 – RELAÇÃO DE VLANS – Segurança das redes	Tabela apresentando as faixas de endereços para várias redes da PRODEB.	Indica existência de iniciativa para a segmentação de redes.

A documentação apresentada indica que existe iniciativa da SAEB para a segmentação de redes, embora não permitam avaliarmos se a segmentação atende às necessidades da entidade.

Opinião da auditoria: diante das evidências encaminhadas, considera-se sanada a irregularidade apontada.

- *Integração entre análise de riscos e política de segurança*

A SAEB informou que a integração depende de investimentos na renovação do contrato de suporte da ferramenta *Risk Manager* e em contratação de serviço de análise de risco da política da segurança da informação junto à PRODEB, portanto a recomendação da auditoria não foi implementada.

Opinião da auditoria: o achado de auditoria deve ser mantido.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

- *Testes de segurança*

A SAEB informou que a realização de testes de segurança depende de investimentos para contratação da PRODEB para execução do serviço, portanto os apontamentos permanecem inalterados.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Análise contínua de riscos relacionados à segurança*

A SAEB informou que a integração depende de investimentos na renovação do contrato de suporte da ferramenta *Risk Manager* e em contratação de serviço de análise de risco da política da segurança da informação junto à PRODEB, portanto os apontamentos da auditoria ficam ratificados.

Opinião da auditoria: o achado de auditoria deve ser mantido.

- *Controle de versão da política de segurança*

Quadro 15 – Análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
10 – RP.2007.077 Política de Segurança_atualizada.	Política de Segurança da PRODEB.	O documento possui uma tabela com registro do histórico de alterações do documento, que foi elaborado em 2007, passou por uma revisão em 2015 e sofreu alteração para inserção de conteúdos em 2017.

Apesar da versão do documento encaminhado possuir uma tabela informando quando sofreu alterações, a PRODEB deve promover um controle mais efetivo das versões da política de segurança aprovadas. Ressaltamos que a última alteração ocorrida na política de segurança da informação foi realizada em 2017, data posterior à realização da auditoria.

Opinião da auditoria: o achado de auditoria deve ser mantido.

RECOMENDAÇÕES:

A seguir serão analisados os esclarecimentos e documentos apresentados pela SAEB a respeito das recomendações sugeridas pela auditoria, relacionadas ao tema Segurança de Sistemas.

Como as evidências apresentadas para as recomendações são praticamente as mesmas apresentadas para as fragilidades, confirmamos o entendimento para as recomendações de 2 a 7. Para a recomendação de número 1 foram apresentadas novos documentos que serão analisados a seguir.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

1. **Aplicar as normas de segurança em todos Os ambientes do Sistemas SIMPAS e Comprasnet.ba.**

Quadro 16 – análise dos documentos apresentados pelos gestores da SAEB

Documento	Do que se trata	Avaliação
10 - NP.AG.2003 – Proteção Contra Códigos Maliciosos	Norma de proteção contra códigos maliciosos.	Evidência de existência da norma, mas não comprova a sua aplicação.
10 - NP.AG.2004 – Uso de Dispositivos Móveis	Norma para utilização de dispositivos móveis no ambiente da PRODEB.	
10 – NP.OP.1001 Backup de dados do data center -v3	Norma que regulamenta o backup e o restore dos dados residentes no Data Center da PRODEB, define padrões, regras e responsabilidades para estas operações.	
10 - NP.AG.2001 – Controle de Acesso ao Data Center PRODEB	Norma que estabelece critérios para acesso e competências específicas, e define procedimentos para controle de acesso de pessoal ao Data Center da PRODEB.	
10 – RP.2007.077 Política de Segurança_atualizada	Política de Segurança da PRODEB.	O documento possui uma tabela com registro do histórico de alterações do documento, que foi elaborado em 2007, passou por uma revisão em 2015 e sofreu alteração para inserção de conteúdos em 2017.

Estes documentos já havia sido apresentados à auditoria que relatou em seu relatório que:

> Foram apresentados documentos referentes a normas permanentes da PRODEB que regulamentam uso de dispositivos móveis, proteção contra código malicioso, backup/restore de dados do Data Center, uso de ferramentas de colaboração, controle de acesso ao Data Center da PRODEB e uso da internet e mídias sociais.

Entretanto, a auditoria informou que esses documentos não comprovam a sua aplicação, relatando inclusive problemas relacionados com a política de backup:

> Contudo na nota técnica da SAEB, de 26/02/2016, foi informado que problemas elétricos ocorridos em 15/01/2016, provocaram interrupção do fornecimento de energia do Data Center, culminando em perda de dados nos servidores que hospedavam os bancos de dados criados para atender essa auditoria. Informou ainda que os dados foram disponibilizados em ambiente de homologação/teste para o qual não existe política de segurança, conforme trecho transcrito a seguir:

Opinião da auditoria: o achado de auditoria deve ser mantido.

CONCLUSÃO

Considerando as novas argumentações e evidências enviadas pela SAEB, foram reavaliados um total de 51 itens, referentes a deficiências relacionadas a seguranças da informação e processos de TI, no que tange às fragilidades identificadas e recomendações presentes no relatório de auditoria do sistema SIMPAS.

Da seção “Deficiências relacionadas à segurança da informação do SIMPAS”, onze recomendações foram reavaliadas e todas mantidas.

Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3
Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.

Para os processos “03-Gerenciamento de Recursos Humanos” e “08-Gerenciamento de Terceirização”, não houve mudança no posicionamento desta auditoria.

O processo “04-Avaliação e gerenciamento de riscos” teve sete das fragilidades apontadas pela auditoria, revisadas. Contudo, a revisão não provocou mudança na opinião desta auditoria. Além disso, quatro recomendações também foram reavaliadas e mantidas para esse processo.

O processo “05-Desenvolvimento e Manutenção de Sistemas” teve seis recomendações reavaliadas, sendo que uma foi suprimida em razão de apresentação de evidência de solução do apontamento de auditoria e as outras cinco foram mantidas.

Para o processo “07-Gerenciamento de Mudanças”, todas as seis recomendações foram reavaliadas e mantidas.

Para o processo “10-Segurança de Sistemas”, foram reavaliadas oito fragilidades apontadas no relatório de auditoria, sendo que sete destas foram mantidas e apenas uma foi suprimida em razão de apresentação de evidência de solução do apontamento de auditoria. Além disso, sete recomendações para esse processo foram reavaliadas e todas mantidas.

Face ao exposto, constata-se que a diligência procedida não teve o condão de alterar o entendimento inicial da Auditoria, exceto no que se refere aos itens 05.1, relativo a necessidade de “*Formalizar metodologia para o processo de desenvolvimento de sistemas*”, e 10.2, “*Respostas da SAEB ao check list de processos, atividades, padrões, boas práticas e controles deli, seção 'SEGURANÇA DE SISTEMAS', que afirmam que os seguintes controles existem, porém não foram fornecidas evidências ou as evidências fornecidas não comprovam a existência do controle*”/”*Segurança de rede - segmentação*”. Deste modo, no que tange aos demais achados, resta ratificado o posicionamento da Auditoria.

Gerência 6A / GATI / SUTEC, 05 de dezembro de 2017.

Este documento foi assinado eletronicamente. As assinaturas realizadas estão listadas em sua última página.
Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3

Quadro de Assinaturas

Este documento foi assinado eletronicamente por:

Alex Pereira dos Santos
Gerente de Auditoria - Assinado em 06/12/2017

Augusto Cesar Pinheiro de Mattos
Gerente - Assinado em 06/12/2017

Augusto Goncalves de Sousa
Gerente - Assinado em 06/12/2017

Karla Maldonado de Oliveira
Analista de Sistemas - Assinado em 07/12/2017

MAURICIO SOUZA FERREIRA
Coordenador de Controle Externo - Assinado em 06/12/2017

Sua autenticidade pode ser verificada no Portal do TCE/BA através do QRCode ou endereço https://www.tce.ba.gov.br/autenticacaocopia, digitando o código de autenticação: M3NZI1MZA3