CEFET/RJ

RELATÓRIO DE AVALIAÇÃO

Divisão de Estratégia e Governança em Tecnologia da Informação

Exercício 2022

20 de agosto de 2022

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA – CEFET/RJ

Auditoria Interna

RELATÓRIO DE AVALIAÇÃO

Órgão: Centro Federal de Educação Tecnológica Celso Suckow da Fonseca

Unidade Examinada: **Divisão de Estratégia e Governança em Tecnologia da Informação - DIGTI**

Município/UF: **Rio de Janeiro/RJ**

Projeto de Auditoria: **Programa de Auditoria 1.b**

Missão

A missão da AUDIN é contribuir - de forma independente - tanto para a avaliação quanto para o aprimoramento do gerenciamento de riscos, dos controles internos e da governança da instituição, além de agregar valor às práticas administrativas e colaborar para a melhoria da gestão quanto à eficácia, eficiência e economicidade dos processos.

Auditoria de conformidade

A auditoria de conformidade visa à obtenção e avaliação de evidências para verificar se as atividades financeiras ou operacionais de um objeto de auditoria selecionado obedecem às condições, às regras e os regulamentos a ele aplicáveis

QUAL FOI O TRABALHO REALIZADO PELA AUDIN DO CEFET-RJ?

Auditoria de Avaliação de conformidade que visa avaliar a adequação das políticas e diretrizes, estrutura e instrumentos de governança de TI às exigências legais.

POR QUE A AUDIN DO CEFET-RJ REALIZOU ESSE TRABALHO?

Em cumprimento ao PAINT 2022, aprovado pela Resolução do CODIR nº 31/2021, este trabalho teve a finalidade de apresentar os resultados da auditoria de conformidade da adequação da gestão de TI às exigências de governança de TI.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDITORIA INTERNA DO CEFET-RJ? QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

Os resultados desse trabalho indicam que a maturidade dos controles apresenta o nível intermediário, constituído por princípios e padrões documentados sobre os controles internos. Entretanto, constatou-se a ausência de documentos estratégicos fundamentais como PDTIC, PETI, a necessidade de atualização de documentos POSIC e o PTD e de designação de servidores para a composição de grupos de trabalho e comitês que deliberem sobre os temas relacionados a PNSI e que atuem na prevenção, tratamento e resposta a incidentes cibernéticos. Com a finalidade de contribuir com a gestão na adequação às exigências de governança de TI, foram produzidas as seguintes recomendações:

1 - Concluir a elaboração do PDTIC e dar publicidade ao mesmo no sítio eletrônico do CEFET-RJ.

2 - Elaborar e publicar as atribuições do COGTI.

3 - Atualizar a composição de membros do COGTI e publicá-la no sítio eletrônico do CEFET-RJ.

4 - Elaborar PETI e dar publicidade ao mesmo no sítio eletrônico do CEFET/RJ.

5 - Providenciar a atualização da POSIC, contemplando a periodicidade das próximas atualizações.

6 - Elaborar plano de ação e de resposta a incidentes sobre a implantação da segurança cibernética

7 - Elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes e submetê-lo ao CGTIC e ao CGRC.

8 - Instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;

9 - Instituir e implementar equipe de prevenção, tratamento e resposta a incidentes.

10 - Promover ações de capacitação no tema segurança da informação preferencialmente aos servidores da área de TI que atuarão nos grupos / comitê/ comissões relativas aos aspectos de segurança da informação – prevenção, tratamento e resposta a incidentes e assuntos relacionados à PNSI.

LISTA DE SIGLAS E ABREVIATURAS

AUDIN	Auditoria Interna do Cefet-RJ
CEFET-RJ	Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
CGRC	Comitê de Governança Riscos e Controle
CGU	Controladoria-Geral da União
CGTIC	Comitê de Governança da Tecnologia da Informação e Comunicação
CODIR	Conselho Diretor
COGTI	Comitê Gestor de Tecnologia da Informação
CSIC	Comissão de Segurança da Informação e Comunicação
CSIRT/DTINF	Grupo de Resposta a Incidentes de Segurança da Informação do Departamento de Tecnologia da Informação do CEFET-RJ
DTINF	Departamento de Tecnologia da Informação
DIGTI	Divisão de Estratégia e Governança em Tecnologia da Informação
EGD	Estratégia de Governo Digital
PAINT	Plano Anual de Auditoria Interna
PDA	Plano de Dados Abertos
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PETI	Plano Estratégico de Tecnologia da Informação e Comunicação
POSIC	Política de Segurança da Informação e Comunicação - Segurança cibernética
PNSI	Política Nacional de Segurança da Informação
PTD	Plano de Transformação Digital
RAINT	Relatório Anual de Atividades da Auditoria Interna
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação
TI	Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação

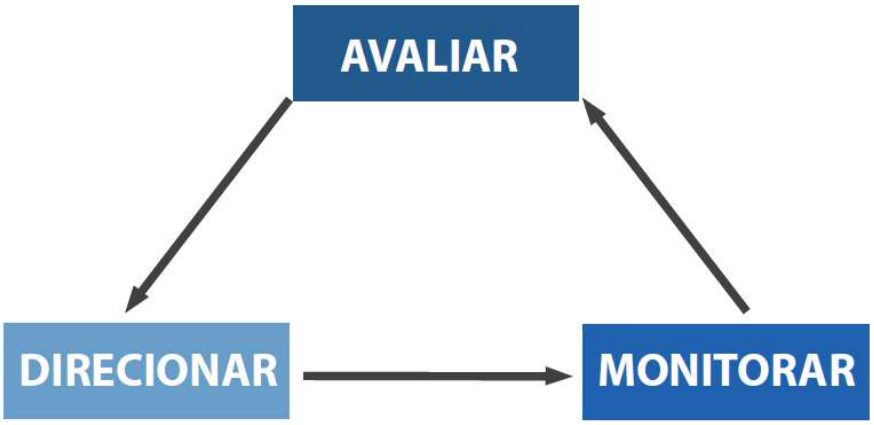
SUMÁRIO

INTRODUÇÃO

Esse relatório objetiva apresentar os resultados da auditoria de conformidade realizada nos meses de julho e agosto de 2022 junto à Divisão de Estratégia e Governança em Tecnologia da Informação – DIGTI do Departamento de Tecnologia da Informação - DTINF, que teve por objeto analisar a adequação da gestão de TI às exigências de governança de TI.

Segundo o Guia de Governança de TIC do SISP, a governança de TIC "é o sistema pelo qual o uso atual e futuro da TIC é dirigido e controlado, mediante avaliação e direcionamento do uso da TIC para dar suporte à organização e monitorar seu uso para realizar os planos, incluída a estratégia e as políticas de uso da TIC dentro da organização". Para a operacionalização da governança, as principais tarefas a serem realizadas pela gestão estão demonstradas na figura a seguir.

Figura 1 – Tarefas da Governança de TIC



Fonte: Adaptado de ABNT, 2015, p. 7.

Assim, considerando o exposto, esta auditoria intentou avaliar o atendimento das exigências legais de governança de TI, em consonância com os ditames: Decreto nº 9.203/2017, Decreto nº 9.637/2018 (PNSI); Decreto nº 9.319/2018 (EGD); Decreto nº 10.332/2020 (EGD 2020-2022); Decreto nº 10.996/2022; Lei nº 14.129/2021 e Portaria nº 778/2019 de maneira a verificar se as exigências estavam sendo cumpridas e de contribuir para melhor desempenho das tarefas relacionadas à governança de TIC.

O escopo da auditoria abrangeu verificar o conjunto basilar de documentos, políticas e diretrizes em consonância às exigências legais de governança de TI, bem como a avaliação da estrutura e instrumentos que forneçam suporte adequado à governança de TI, especialmente nos aspectos relativos a segurança da informação e a transformação digital.

Origem e justificativa

A auditoria decorreu da avaliação do gerenciamento de risco e controle interno realizado pela Audin do CEFET/RJ ante aos objetivos institucionais, para a definição do PAINT 2022, quando se identificou alto risco associado à atividade. Cabe ressaltar diversos processos conduzidos pela área de governança de TI demandam além de demandarem conhecimento técnico específico perpassam por várias áreas que envolvem algumas divisões do DTINF e outras Divisões/Diretorias no âmbito do Cefet-RJ. No concernente à auditoria interna, o processo se dá de modo a averiguar se as os dispositivos legais e normativos internos e os documentos norteadores estratégicos encontram-se elaborados, vigentes e em conformidade com os preceitos legais, emitindo, ao final, relatórios de recomendação.

Objetivo e questões de auditoria

Com a finalidade de examinar as atividades e os processos relativos de governança de TI, o trabalho buscou responder as seguintes questões:

1. Existem políticas e diretrizes definidas para governança e gestão de TIC?
2. Há estrutura e instrumentos de governança que deem suporte adequado à governança de TIC considerando a Segurança da Informação e a transformação digital?
3. Os controles internos relativos à governança de TIC estão adequados?

Metodologia

A metodologia empregada com a finalidade de obter evidências razoáveis e suficientes, responder às questões de auditoria e fundamentar as conclusões e recomendações para a administração da entidade, consistiu na realização dos procedimentos de análise documental por meio da avaliação dos documentos obtidos em resposta às indagações escritas através solicitações de auditoria e os que tiveram como fontes de informação os sítios governamentais, os documentos e normativos internos do Cefet/RJ, e a legislação pertinente acerca do tema da auditoria.

A fim de analisar as atividades da Instituição relativas à governança de TI, inicialmente, após a reunião de abertura dos trabalhos, foi questionada a existência dos seguintes documentos: PDTIC, PETI, PTD; se havia designação de responsável pelo planejamento da segurança cibernética; Plano de ação e respostas a incidentes críticos conforme POSIC, tais questionamentos foram realizados por meio da emissão da SA n° 1.b_01, solicitando além dos documentos já mencionados, informações sobre COGTI e CGTIC.

Em seguida, foi emitida a SA nº 1.b_02 requerendo: comprovante de designação do gestor da segurança da informação; esclarecimentos sobre CSIC e CSIRT/DTINF; informações sobre ações de capacitação sobre segurança da informação.

Posteriormente foram emitidas as SA nº 1.b_03 solicitando: confirmação se o que estava previsto para ser realizado do PTD até dez/2021 foi executado e qual status das atividades previstas para serem concluídas em ou e dez/2022; informações sobre a

atualização da Base Nacional de Serviços Públicos e da Plataformas de Governo Digital; confirmar se a minuta de Regimento do COGTI foi aprovada pela DIREG e a SA nº 1.b_04 requerendo: confirmação se o PTD havia sido aprovado pelo COGTI ou CGTIC ou pelo Dirigente máximo da instituição e solicitando informações se o PTD já havia sido encaminhado para a aprovação ou se já estava aprovado pela Secretaria de Governo Digital da Secretaria de Desburocratização, Gestão e Governo Digital do Ministério da Economia.
Adicionalmente foram realizados os seguintes procedimentos de auditoria: verificação do diagnóstico situacional encaminhado pela unidade auditada, análise dos fluxos/mapas de processos encaminhados pela unidade auditada, elaboração da matriz de riscos e controles e da matriz de achados.

Restrições/Limitações

Não houve restrição ou limitação ao processo de auditoria a ser registrado.

Considerações Iniciais

Os resultados desse trabalho permitiram identificar que a maturidade dos controles apresenta o nível intermediário, constituído por princípios e padrões documentados sobre os controles internos. Contudo, constatou-se a ausência de documentos fundamentais para a estratégia de governança de TI como PDTIC, PETI – o que caracteriza a inobservância das exigências legais e impacta o direcionamento das atividades de TI conforme as estratégias organizacionais. Verificou-se também a necessidade de atualização e/ou emissão de nova versão como a POSIC e o PTD e de designação de servidores para a composição de grupos de trabalho e comitês que deliberem sobre os temas relacionados a PNSI e que atuem na prevenção, tratamento e resposta a incidentes cibernéticos.

RESULTADOS DOS EXAMES

Apresentam-se, a seguir, as constatações em relação ao objeto auditado e suas respectivas análises.

1. Não há Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC vigente

Contextualização
Conforme disposto no art. 6º da Portaria nº 778 de 2019, o Plano Diretor de TIC - PDTIC é o instrumento de alinhamento entre as estratégias e os planos de TIC e as estratégias organizacionais.
No âmbito do Cefet/RJ, o PDTIC costuma acompanhar a periodicidade do PDI, com vigência atual para o período de 2020-2024. Contudo, o último PDTIC disponível, aprovado e publicado para o Cefet/RJ, teve a vigência finda em 2019.
Por meio da pesquisa ao sítio eletrônico do Cefet-RJ, não foi identificado PDTIC vigente, foi realizada a indagação escrita via SA 1.b_01, na qual solicitou-se o envio do PDTIC e em resposta, a DIGTI informou que "O PDTIC (Plano Diretor de Tecnologia da Informação e Comunicação) esta andamento, falta terminar o plano de metas e ações, as ações priorizadas para 2023 e elaborar o plano orçamentário."

Condição
Ausência de PDTIC aprovado e formalizado

Critério
PDTIC aprovado, publicado e vigente

Causa
PDTIC não foi elaborado tempestivamente

Consequência
Possíveis falhas no alinhamento entre as estratégias e os planos de TIC e as estratégias organizacionais.

Conclusão
O PDTIC é um documento basilar no aspecto estratégico e norteador para o planejamento das atividades e projetos na área de Tecnologia da Informação, a ausência de elaboração do mesmo esmorece o alinhamento entre as estratégias e os planos de

TIC e as estratégias organizacionais. Destaca-se, portanto, através do achado a necessidade de conclusão, o mais breve possível, da elaboração e a publicação do PDTIC.

2. Não há Plano Estratégico de Tecnologia da Informação e Comunicação - PETI no âmbito do Cefet-RJ

Contextualização

Assim como o PDTIC, o PETI é um dos documentos orientadores da estratégia de TI no âmbito do Cefet/RJ.

A aprovação do mesmo é de responsabilidade do CGTIC e costuma acompanhar o período de vigência do PDTIC e ser um documento de alinhamento entre o PDI, o PDTIC e as estratégias organizacionais e de TI.

Por meio da pesquisa ao sítio eletrônico do Cefet-RJ, não foi identificado PETI vigente, foi realizada a indagação escrita via SA 1.b_01, na qual solicitou-se o envio do PETI e em resposta, a DIGTI informou que "O PETIC (Plano Estratégico de Tecnologia da Informação e Comunicação) ainda não foi elaborado, mas consta no levantamento de necessidades identificadas do PDTIC."

Condição

Ausência de PETI aprovado e formalizado

Critério

PETI aprovado, publicado e vigente

Causa

PETI não foi elaborado tempestivamente

Consequência

Possíveis falhas no alinhamento entre as estratégias e os planos de TIC.

Conclusão

O PETI é um documento dos documentos orientadores do planejamento das atividades e projetos na área de Tecnologia da Informação, a ausência de elaboração do mesmo pode fragilizar o alinhamento entre as estratégias e os planos de TIC e as estratégias organizacionais. Assim, através do achado, ressalta-se a necessidade de conclusão, o mais breve possível, da elaboração e a publicação do PETI.

3. Não há item relativo a segurança e privacidade e estratégias de monitoramento no Plano de Transformação Digital – PTD

Contextualização

O Plano de Transformação Digital – PTD possui conteúdo mínimo estabelecido no inciso I e no § 3º do Art. 3º do Decreto nº 10.332 de 2020.

Por meio da pesquisa ao sítio eletrônico do Cefet-RJ, inicialmente não foi identificado nenhum documento relativo ao PTD, mas havia uma página ligada ao Departamento de Tecnologia da Informação – DTINF com as informações a respeito do PTD e uma tabela de atividades relacionadas à transformação digital. Foi realizada a indagação oral sobre referido documento e indagação escrita via SA 1.b_01, em resposta, a DIGTI informou que "O PTD (Plano de transformação Digital) foi publicado na página do DTINF."

Posteriormente foi arguida via SA 1.b_03 se as atividades relativas à transformação digital que tinham o prazo definido para Dez/21 haviam sido concluídas e o status da que estavam para vencer em out e dez/22, como resposta a DIGTI informou que relativamente aos serviços previstos para dez 21 " Todos os serviços foram concluídos." E quanto aos serviços cuja conclusão estava prevista para 2022 "Todos os serviços estão em andamento e no prazo".

Observou-se que o PTD não continha timbre oficial, não estava assinado e aparentou conter as orientações relativas ao seu preenchimento/envio. Ademais dentre os itens mínimos estabelecidos, não foram identificadas as ações relativas à segurança e a privacidade e no que tange aos itens unificação de canais digitais e interoperabilidade de sistemas, apesar do PTD contemplar os referidos itens, não foram identificadas quais seriam as ações estabelecidas e previstas para cada um desses itens.

Condição

Ausência de item exigido legalmente e de estratégias de monitoramento no PTD

Critérios

- PTD aprovado pelo CGTIC e publicado
- PTD aprovado pela Secretaria de Governo Digital da Secretaria de Desburocratização, Gestão e Governo Digital do Ministério da Economia
- PTD contempla os elementos mínimos previstos no Decreto nº 10.332/2020
- PTD contempla estratégias de monitoramento conforme previsto no Decreto nº 10.332/2020

Causa

Inobservância das exigências legais quando da elaboração do PTD

Consequência
Possível falha cumprimento das exigências, dos objetivos e das metas de transformação digital dada aos órgãos pelo governo federal.

Conclusão
O PTD é um instrumento de planejamento para a consecução dos objetivos estabelecidos na Estratégia de Governo Digital, conforme Art. 3º do Decreto nº 10.332 de 2020. Contudo, considerando que os prazos estabelecidos no documento estão findando (dezembro/2022), que a legislação que institui os requisitos legais se refere ao interstício temporal de 2020-2022, apesar das incompletudes observadas no mesmo, não se considera razoável a alteração do referido documento neste momento. Salienta-se, todavia, a orientação de que sejam observadas todas as exigências legais caso haja nova previsão legal de elaboração de PTD para um próximo período, seja através de uma EGD 2023-2025, ou documento similar.

4. Política de Segurança da Informação - POSIC desatualizada e sem medidas de monitoramento e controle

Contextualização
A elaboração da Política de Segurança da Informação – POSIC é uma determinação legal oriunda do Decreto nº 9637 de 2018. Verificou-se que algumas das recomendações da auditoria realizada anteriormente foram relativas a elaboração da POSIC e a designação de servidor/equipe responsável pela segurança cibernética visando a implantação da PNSI, conforme previsto no referido ditame.
Analisando o documento publicado em 2018 e a fim de verificar a conformidade com as exigências da legislação vigente, emitiu-se a SA 1.b_01 averiguando se havia designação de servidor responsável pelo planejamento da segurança cibernética e a respeito Plano de ação e de resposta a incidentes sobre a implantação da segurança cibernética e relatórios anuais (2020 e 2021) a respeito da implementação da segurança cibernética, conforme previsto no POSIC. Foram solicitados esclarecimentos. Em resposta a DIGTI informou que “Foi elaborado o documento formalizando a designação do servidor Marcus Vinicius dos Santos como gestor da Segurança da informação. O documento será tramitado à direção geral. (...) Não foi elaborado o plano de ação e de resposta a incidentes e nem relatórios a respeito da implementação da segurança cibernética pois iremos elaborar uma nova Política de Segurança do Cefet/RJ.”

Condição
POSIC desatualizada e com instrumentos de monitoramento e controle não implantados.

Critério

Ações de controle e monitoramento previstas na POSIC e na PNSI em execução.

Causa
Inobservância das exigências legais vigentes quando da elaboração e/ou atualização da POSIC.

Consequência
Possível falha na estruturação e operacionalização das atividades relativas à segurança da informação com consequente vulnerabilidade dos sistemas e das informações institucionais à ataques cibernéticos e desacordo e não cumprimento de exigências legais.

Conclusão
Contatou-se que, embora haja POSIC publicada, o fato do servidor responsável pela segurança da informação cibernética ter sido designado durante o procedimento de auditoria e a observação de que os instrumentos de controle e monitoramento – como o plano de ação e de resposta a incidentes sobre a implantação da segurança cibernética e os relatórios anuais sobre a implementação do plano de ação não terem sido elaborados, demonstra uma fragilidade tanto na estrutura quanto nos controles internos.

5. Não há comitê de segurança da informação ou estrutura equivalente para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação - PNSI no âmbito do Cefet/RJ

Contextualização
A elaboração da Política de Segurança da Informação – POSIC é uma determinação legal oriunda do Decreto nº 9637 de 2018 que em seu Inciso IV, Art. 15 dispõe que os órgãos e entidades da administração pública federal deverão instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI. Analisando o documento publicado em 2018 e a fim de verificar a conformidade com as exigências da legislação vigente, emitiu-se a SA 1.b_02 de modo a esclarecer se a Comissão de Segurança da Informação e Comunicação – CSIC havia sido constituída e se encontrava em funcionamento. Em resposta a DIGTI informou que “Ainda não foi instituída a CSIC nem o CSIRT/DTINF. Ambas estão em processo de elaboração.”

Condição
Não há designação de servidores para composição da CSIC no âmbito do Cefet-RJ.

Critério
CSIC designada e em operação.

Causa
Inobservância dos dispositivos legais e normas internas vigentes.

Consequência
Possível falha na estruturação e operacionalização das atividades relativas à segurança da informação com consequente vulnerabilidade dos sistemas e das informações institucionais à ataques cibernéticos e desacordo e não cumprimento de exigências legais.

Conclusão
Apesar da POSIC publicada, percebe-se falhas na estruturação recomendada pela PNSI visto que não há designação de comitê de segurança da informação ou estrutura equivalente para deliberar sobre os assuntos relativos à Política Nacional de Segurança da Informação - PNSI no âmbito do Cefet/RJ, o que pode acarretar vulnerabilidade dos controles internos e possibilitar a ocorrência de exposição a incidentes cibernéticos.

6. Não há equipe designada para atuar na prevenção, no tratamento e na resposta a incidentes cibernéticos

Contextualização
A elaboração da Política de Segurança da Informação – POSIC é uma determinação legal oriunda do Decreto nº 9637 de 2018 que em seu Inciso VII, Art. 15 dispõe que os órgãos e entidades da administração pública federal deverão instituir e implementar equipe de prevenção, tratamento e resposta a incidentes cibernéticos.
Analisando o documento publicado em 2018 e a fim de verificar a conformidade com as exigências da legislação vigente, emitiu-se a SA 1.b_02 de modo a esclarecer se o Grupo de Resposta a Incidentes de Segurança da Informação do Departamento de Tecnologia da Informação do CEFET/RJ - CSIRT/DTINF havia sido constituído e se encontrava em funcionamento. Em resposta a DIGTI informou que “Ainda não foi instituída a CSIC nem o CSIRT/DTINF. Ambas estão em processo de elaboração.”

Condição
CSIRT/DTINF não instituído no âmbito do Cefet/RJ.

Critério
CSIRT/DTINF designado e em operação.

Causa

Inobservância dos dispositivos legais e normas internas vigentes.

Consequência
Possível falha na estruturação e operacionalização das atividades relativas à segurança da informação com consequente vulnerabilidade dos sistemas e das informações institucionais à ataques cibernéticos e desacordo e não cumprimento de exigências legais.

Conclusão
Apesar da POSIC publicada, percebe-se falhas na estruturação recomendada pela PNSI visto que não há designação de equipe designada para atuar na prevenção, no tratamento e na resposta a incidentes cibernéticos no âmbito do Cefet/RJ, o que pode acarretar vulnerabilidade nos aspectos relativos a segurança da informação.

7. Não foram realizadas ações de capacitação relacionadas ao tema segurança da informação para os servidores a nível institucional.

Contexto da auditoria
A elaboração da Política de Segurança da Informação – POSIC é uma determinação legal oriunda do Decreto nº 9637 de 2018 que em seu Inciso VI, Art. 15 dispõe que os órgãos e entidades da administração pública federal promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à segurança da informação.
Analisando o documento publicado em 2018 e a fim de verificar a conformidade com as exigências da legislação vigente, emitiu-se a SA 1.b_02 de modo a esclarecer se foram realizadas ações de capacitação e profissionalização dos servidores do DTINF em temas relacionados à segurança da informação, bem como se houveram ações de capacitação ou informativas a nível institucional (para os demais servidores do CEFET/RJ) a respeito do tema. Em resposta a DIGTI enviou uma tabela com a descrição de capacitações realizadas por alguns servidores de unidades e 4 servidores do DTINF/Maracanã acerca do tema.

Condição
Não foram realizadas ações de capacitação relacionadas ao tema segurança da informação tanto para os servidores que atuam na área de TI quanto para os servidores a nível institucional.

Critério

Ações de Capacitação relacionadas ao tema segurança da informação promovidas tanto para os servidores que atuam na área de TI quanto para os servidores a nível institucional.

Causa
Inobservância dos dispositivos legais e normas internas vigentes.

Consequência
Possível falha na estruturação e operacionalização das atividades relativas à segurança da informação com consequente vulnerabilidade dos sistemas e das informações institucionais à ataques cibernéticos e desacordo e não cumprimento de exigências legais.

Conclusão
Para que a PNSI seja implantada, devidamente planejada, elaborada e operacionalizada com os instrumentos de controle e monitoramento previstos na legislação, se faz necessário a capacitação dos servidores que atuarão diretamente com os instrumentos da PNSI e uma sensibilização institucional a respeito do tema de modo a sensibilizar e esclarecer os servidores sobre o tema.

RECOMENDAÇÕES

Recomendações para DTINF

1 - Concluir a elaboração do PDTIC e dar publicidade ao mesmo no sítio eletrônico do CEFET-RJ.

Achado n° 1

Recomendações para DIREG

2 - Elaborar e publicar as atribuições do COGTI.

Achado n° 1

3 - Atualizar a composição de membros do COGTI e publicá-la no sítio eletrônico do CEFET-RJ.

Achado n° 1

Recomendações para DTINF

4 - Elaborar PETI e dar publicidade ao mesmo no sítio eletrônico do CEFET/RJ.

Achado n° 2

Recomendações para Gestor de Segurança da Informação

5 - Providenciar a atualização da POSIC, contemplando a periodicidade das próximas atualizações.

Achado n° 4

6 - Elaborar plano de ação e de resposta a incidentes sobre a implantação da segurança cibernética

Achado n° 4

7 - Elaborar relatório anual sobre a implementação do plano de ação e de resposta a incidentes e submetê-lo ao CGTIC e ao CGRC.

Achado n° 4

Recomendações para DIREG

8 - Instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;

Achado n° 5

9 - Instituir e implementar equipe de prevenção, tratamento e resposta a incidentes.

Achado n° 6

Recomendações para DTINF

10 - Promover ações de capacitação no tema segurança da informação preferencialmente aos servidores da área de TI que atuarão nos grupos / comitê/ comissões relativas aos aspectos de segurança da informação – prevenção, tratamento e resposta a incidentes e assuntos relacionados à PNSI.

Achado n° 7

CONCLUSÃO

A partir das análises realizadas, considerando os aspectos relativos aos riscos e controles, identifica-se que o nível de maturidade dos controles da adequação da gestão de TI às exigências de governança de TI é classificado como intermediário, ou seja, identifica-se que há princípios e padrões documentados sobre os controles internos.

Contudo, no transcorrer do presente trabalho de auditoria, considerando os achados apresentados e as questões de auditoria elaboradas para o trabalho que há ausência de elaboração de documentos basilares e estratégicos como o PDTIC e o PETI e que alguns documentos que estão vigentes, como o PTD e a POSIC necessitam de atualização e ajustes/reformulação. Há fragilidades na estruturação e nas atividades de monitoramento e controle relativos especialmente à segurança cibernética.

A intenção dos resultados apresentados neste relatório, é a de contribuir com a implementação de estruturação, controles e melhoria dos processos relacionados à governança de TI no âmbito do CEFET/RJ

SHEILA DA SILVA CARVALHO SANTOS:08870963799

Assinado de forma digital por SHEILA DA SILVA CARVALHO SANTOS:08870963799
Dados: 2022.09.12 12:16:09 -03'00'

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO

DE ACORDO:

RAFAEL RAYMUNDO DE SANTANA:05669624700

Assinado de forma digital por RAFAEL RAYMUNDO DE SANTANA:05669624700
Dados: 2022.09.12 12:21:00 -03'00'