RELATÓRIO DE AUDITORIA INTERNA Nº 04/2023

Setor de Tecnologia da Informação

Florianópolis – Santa Catarina

2023

I. INTRODUÇÃO

Em cumprimento ao Plano Anual de Atividades de Auditoria Interna – PAINT 2023, apresenta-se o Relatório Preliminar de Auditoria Interna sobre o Setor de Tecnologia da Informação. Este trabalho de auditoria interna contém o resultado dos trabalhos de avaliação efetuados no que diz respeito ao TI, tomando-se como base o disposto na legislação que rege o tema.

O trabalho foi realizado no período de 26/07/2023 à 15/08/2023, sendo executado de acordo com os procedimentos de auditoria geralmente aceitos, na extensão julgada necessária às circunstâncias apresentadas e não houve restrição aos exames.

Em 26/07/2023 foi realizada a reunião de abertura com a presença do controlador interno e do Supervisor do Setor de Tecnologia da Informação, com o objetivo de colher informações para a preparação da documentação de auditoria.

No período do dia 26/07/2023 à 11/08/2023 foram colhidos dados acerca da gestão do Setor de TI. Nenhuma restrição foi imposta quanto ao método ou extensão dos trabalhos. Os procedimentos para execução dos exames de auditoria foram aplicados de acordo com a natureza e atividade da unidade auditada e abrangeram suas áreas de atuação.

II. OBJETIVOS

Fornecer subsídios suficientes para os gestores avaliarem se o Setor está alcançando os resultados planejados, através do acompanhamento e verificação das atividades. Visando, com isso, reduzir os riscos de falhas nos processos internos, que possam impactar a missão do CRM-SC.

III. BASE NORMATIVA

a) Constituição Federal e Leis:

- Constituição Federal/88 - Arts. 70 e 74;
- Emenda Constitucional nº 19/98;
- Lei nº 4.320/64 - Lei de Finanças Públicas;
- Lei nº 8.666/93 - Lei de Licitações e Contratos Administrativos;
- Lei Complementar nº 101/00 - Lei de Responsabilidade Fiscal;
- Lei nº 14.133/21 – Nova Lei de Licitações e Contratos Administrativos;
- Lei nº 14.129/2021 - Princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados.

b) Decretos:

- Decreto-Lei nº 200/1967 - Organização Administrativa Federal;
- Decreto nº 1.171/1994 - Código de Ética do Servidor Público Civil;
- Decreto nº 3.591/2000 - Sistema Controle Interno do Governo Federal;
- Decreto nº 7.892/2013 - Sistema de Registro de Preços;

- Decreto n° 9.203/2017 - Política de governança da administração pública federal direta, autárquica e fundacional;

c) Resoluções e Manuais:

- Resolução CFM nº 2.151/2016 - Regras e conteúdos para o acesso a informações, no âmbito dos Conselhos de Medicina, de que trata a Lei n° 12.527, de 18 de novembro de 2011;
- Resolução CFM nº 2.286/2020 - Normas e procedimentos para tomada e prestação de contas dos Conselhos de Medicina;
- Resolução CRM-SC nº 206/2021 - Aprova alteração do Regimento Interno do Conselho Regional de Medicina do Estado de Santa Catarina, previsto pela Resolução CRM-SC Nº 198/2020;
- Resolução CRM-SC nº 215/2022, que cria a Controladoria Interna do Conselho Regional de Medicina do Estado de Santa Catarina.

d) Normas brasileiras profissionais e técnicas aplicadas à auditoria interna:

- Resolução CFC nº 781/1995. NBC PI 01 - Normas Profissionais do Auditor Interno;
- Resolução CFC nº 986/2003. NBC TI 01 - Da Auditoria Interna;
- Resolução CFC nº 1.229/2009. NBC TA 610 – Utilização do Trabalho de Auditoria Interna;
- Resolução CFC nº 1.311/2010. NBC PA 290 – Independência - Trabalhos de Auditoria e Revisão.

e) Normas de segurança da informação:

- ISO/IEC 27001: Especifica os requisitos para estabelecer, implementar, manter e melhorar um sistema de gestão de segurança da informação (SGSI) em uma organização;
- ISO/IEC 27002: Fornece diretrizes detalhadas para a implementação de controles de segurança da informação recomendados pela ISO 27001;
- COBIT (Control Objectives for Information and Related Technologies): Framework que oferece uma estrutura de governança e gerenciamento de TI, auxiliando na compreensão e gerenciamento dos riscos associados à TI.

f) Instruções normativas:

- Instrução Normativa CGU nº 05/2021 - Plano Anual de Auditoria Interna, sobre o Relatório Anual de Atividades de Auditoria Interna e sobre o parecer sobre a prestação de contas da entidade das unidades de auditoria interna governamental;
- Instrução Normativa CGU nº 04/2018 - Sistemática de Quantificação e Registro dos Resultados e Benefícios da Atividade de Auditoria Interna Governamental do Poder Executivo Federal;

- Instrução Normativa TCU n° 84/2020 - Normas para a tomada e prestação de contas dos administradores e responsáveis da administração pública federal, para fins de julgamento pelo Tribunal de Contas da União;
- Decisão Normativa TCU n° 198/2022 - Normas complementares para a prestação de contas dos administradores e responsáveis da administração pública federal;
- Instrução Normativa CGU nº 10/2020 - Sistemática de Quantificação e Registro dos Resultados e Benefícios da Atividade de Auditoria Interna Governamental do Poder Executivo Federal;
- Instrução Normativa Conjunta MP/CGU nº 01/2016 - Procedimentos para gerir os riscos, proteger a integridade das instituições e a segurança dos recursos públicos.

QUESTÕES DE AUDITORIA;

Com vistas a realizar testes de observância nos controles internos, foram elaboradas 16 (dezesseis) questões de Auditoria sobre temas relevantes referentes à TI, as quais foram respondidas pelos responsáveis da unidade auditada. Cada questão possui requisitos que foram verificados e testados pela equipe de auditoria.

Abaixo, segue a lista de questões com suas respectivas respostas:

Questão nº 01: Existem políticas e normas de TI descritas, aprovadas e divulgadas?
Resposta: Atualmente o setor de TI segue as boas práticas baseadas nas normas SO/IEC 27000, ISO/IEC 270001, ISO/IEC 27002 e na LPGD.

Questão nº 02: Há normas/políticas de segurança para a conduta adequada quanto ao manuseio, controle e proteção das informações?
Resposta: Segue as boas práticas baseada na LPGD.

Questão nº 03: Há diretrizes quanto ao uso da internet? Há formulário específico para a orientação do usuário quanto à utilização da internet?
Resposta: Todo colaborador ao entrar no CRMSC deve assinar com visto de ciência o TERMO DE RESPONSABILIDADE PELO USO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO, este termo indica as responsabilidades e restrições que deve seguir. (adicionado em anexo neste processo)

Questão nº 04: Há controle de equipamentos de terceirizados utilizados pelo Conselho com informações sobre especificação do item, valor, disposição, manutenções ou chamados?
Resposta: Todos os equipamentos de uso terceirizados estão sobre contrato comodato, do qual foram contratados via pregão, atualmente nesta categoria o CRMSC tem apenas o aluguel ara uso de impressoras Laser Mono/Coloridas.

Questão nº 05: As manutenções de rotina semestrais do parque computacional são feitas? É emitido relatório das atividades com resultados e problemas encontrados?

Resposta: Visando o máximo desempenho foi implantado no CRMSC o conceito de realizar a compra de novos computadores (na categoria notebook), do qual os mesmos têm garantia direto do fabricante de 60 meses (5 anos), após esse período os respectivos equipamentos serão leiloados e em paralelo seria realizado a compra de novos notebooks. Saliento que, existe alguns computadores que estão no padrão All In One, porem são máquinas que atualmente estão sendo usadas em caráter temporário (já que tais equipamentos serão dados baixa) até a chegada de novos notebooks.

Questão nº 06: As verificações diárias do servidor são feitas? É emitido relatório das atividades com resultados e problemas encontrados?

Resposta: O acesso aos servidores é diário, problemas pontuais são registrados no sistema de chamados interno IT Manager.

Questão nº 07: Há manutenção e acompanhamento dos sistemas? Foram emitidos relatórios sobre esse acompanhamento, problemas e soluções encontradas?

Resposta: Todos os sistemas que são desenvolvidos pelo CRMSC são realizados por uma empresa terceirizada de desenvolvimento do qual nos encaminha relatórios mensais de melhorias e correções nestes sistemas.

Questão nº 08: Há controle dos indicadores de disponibilidade por falhas dos sistemas utilizados?

Resposta: Temos registro de falhas e ocorrências, porém não temos indicadores.

Questão nº 09: Há controle dos prestadores de serviço e avaliação dos serviços prestados na área de TI?

Resposta: Todos os prestadores de serviços são pagos mensalmente por seus serviços realizados mediante aos processos SGED aberto para cada demanda, questionamentos pontuais são levantados sempre que apontados pelo fiscal do contrato antes de autorizar o pagamento. Avaliação é feita no mesmo processo, assim permitindo dar sequência no contrato, caso não estejam prestando serviços de qualidade, todo o contrato junto ao CRMSC existe uma cláusula do qual permite ao órgão cancelar este contrato caso seja necessário e de interesse do CRMSC.

Questão nº 10: Os acessos aos processos sigilosos são controlados? Somente os servidores indicados possuem acesso aos processos sigilosos?

Resposta: Todos os processos e documentação importantes do setor de TI estão sobre o controle do setor, que pode compartilhar com outros setores quando necessários. Quanto ao sistema gerenciado pelo setor de TI, as liberações de acessos são realizadas mediante o pedido formal da direção, coordenação ou supervisão do respectivo setor, não cabe ao setor de TI definir os indicados nos processos do qual não responde diretamente, apenas controla o fluxo dos acessos.

Questão nº 11: Com que frequência são realizadas cópias de segurança de dados (backup)? Qual tipo de backup é utilizado?

Resposta: São realizados backup de segunda-feira a sexta-feira, realizando backup diárias FULL e incrementais, assim como é realizado backup semanais, além de backup mensais, aonde a organização e controle de backup atual permite o arquivamento de arquivos criados e documentos dos mais diversos pelo período de 1 (um) ano, e documentos digitalizados PDF por 1(um) mês. Os backups são arquivados em disco de backup externo e unidade de fita de backup que são arquivadas em cofre dentro do CRMSC.

Questão nº 12: Quais medidas são adotadas para segurança da informação? São feitos relatórios de acompanhamento de quebras na segurança e planos de ação para melhorias?

Resposta: segue as boas práticas baseada na LPGD, para quebras de segurança são abertos processos a fim de periciar a questão e solucionar o caso. As ações de melhorias são focadas na instrução dos usuários que é um elo importe para a segurança como a própria LGPD define. O setor de TI tenta manter sempre os sistemas atualizados (sistemas operacionais, antivírus corporativos, e sistemas próprios do CRMSC) visando a segurança continuada.

Questão nº 13: Há plano de capacitação para os profissionais de TI? Os servidores buscam atualização profissional?

Resposta: Não existe mais devido à continua mudança da direção, porem com a antiga direção tivemos projetos para implantar o Power BI, Itil e Cobit. Os servidores buscam continua atualização profissional, como novas graduações/formações/especializações, porém são gastos oriundos dos próprios colaboradores sem apoio do CRMSC.

Questão nº 14: Há projetos ou planejamentos que visem inovação tecnológica?

Resposta: Atualizamos o data center CRMSC com novos servidores mais modernos, ainda para o ano de 2023 está prevista a mudança do sistema de telefonia tradicional e atual para VOIP, temos a projeção futura de melhoria no serviço de WIFI e atualização dos sistemas/softwares usados por verões mais recentes, porem a projeção orçamentária disponível para o próximo ano que irá definir o que poderemos ou não fazer.

Questão nº 15: Há planejamento para aquisição de bens para manutenção e/ou melhoria da infraestrutura de TI?

Resposta: Atualizamos o data center CRMSC com novos servidores mais modernos, demais itens como WIFI com melhor desempenho irá depender da projeção orçamentária disponível para o próximo ano que irá definir o que poderemos ou não fazer.

Questão nº 16: Há segurança no Data Center?

Resposta: Sim, o mesmo fica limitado o controle e acesso apenas para o setor de TI, aonde a mesma tem porta com fechadura eletrônica que depende de senha ou digital para controle de acesso, o ambiente é climatizado, com equipamentos de segurança e proteção dentro do setor/data center.

IV. ACHADOS DE AUDITORIA;

Os achados de auditoria são constatações que advêm de impropriedades detectadas nos trabalhos de campo. Cada achado de auditoria gera recomendações a serem implementadas pelo gestor.

A seguir, serão relatados os achados de auditoria e suas respectivas recomendações.

Achado nº 01: Ausência de manuais de procedimentos internos.

A Tecnologia da Informação tem um papel importante na viabilização das estratégias de qualquer organização pública. Para que a TI possa suportar, adequadamente, a Cadeia de Valor da Entidade e implementar, da forma mais assertiva possível, as melhores soluções tecnológicas disponíveis, é necessário que a unidade de TI possua um alto nível de maturidade quanto ao modelo de processos adotado.

E para garantir uma cobertura adequada aos processos, a TI deverá disponibilizar um modelo sistêmico que esteja alinhado às necessidades da organização e que provenha um bom funcionamento de todas as estruturas.

Dessa forma, a elaboração de manual de procedimentos é essencial, visto que orientará a atuação de todos os colaboradores da referida unidade, bem como facilitará o controle interno.

Destaca-se que o manual de procedimentos é um documento que fornece informações sobre as diferentes operações realizadas. É elaborado pelo departamento onde é utilizado e apresenta suas informações de forma detalhada, ordenada, sistematizada e compreensível.

Os manuais de procedimento têm como objetivo: Facilitar o treinamento da equipe; fornecer uma visão abrangente dos processos que compõem o trabalho do departamento; permitir avaliar o desempenho dos trabalhadores com base no ideal esperado pela organização.

Os procedimentos serão revistos sempre que se justifique. Seja por novos procedimentos, ou ajustes aos existentes. É recomendável que pelo menos uma vez por ano seja revisto. É normal existirem alterações ao longo de um ano, ainda que mínimas, e que não as espelhemos de imediato no manual. Ao relê-lo temos a oportunidade de o atualizar. Assim se garante a coerência entre o que está definido (manual) e o que se faz na prática.

Recomendação nº 01: Recomenda-se ao Setor de TI elaborar manuais de procedimentos internos que englobem todas as atividades, bem como definam as responsabilidades de todos os envolvidos.

Prazo: Fevereiro/2024

Achado nº 02: Não há políticas e normas de TI no CRM-SC que defina as diretrizes para a Segurança da Informação.

Com o crescente aumento do uso da Internet, surgem preocupações diretamente ligadas aos dados ou informações de uma Instituição, assim, com o avanço dessa ferramenta em suas diversas formas de utilização, faz-se necessário uma Política que defina as diretrizes para a Segurança da Informação, para garantir a integridade, confidencialidade e disponibilidade das informações sob responsabilidade de uma Instituição.

Muitos riscos de segurança da informação podem surgir da ausência de estruturas apropriadas, processos e políticas, como: a apropriação indevida de ativos, informações confidenciais de acesso não autorizado, vulnerabilidade a ataques lógicos e físicos, indisponibilidade e ruptura de informações, mau uso da informação, não conformidade com leis e regulamentos sobre dados pessoais além de falhas na recuperação de desastres.

A Política de Segurança da Informação deve definir os ativos organizacionais (dados, equipamentos, processos de negócio) que precisam de proteção assim como procedimentos, ferramentas e controles de acesso físico que protejam tais ativos (INTOSAI, 2016).

Uma Política de Segurança descreve a conduta adequada para o manuseio, controle e proteção das informações, contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentalmente ou intencionalmente.

Esta Política se aplicará às informações sob responsabilidade do Conselho Regional de Medicina do Estado de Santa Catarina – CRM-SC, em qualquer forma ou meio que a informação seja apresentada ou compartilhada, que deverão estar sempre protegidas adequadamente, de acordo com controles definidos nesta política.

O cumprimento desta Política de Segurança será acompanhado e auditado pelo setor de Informática do CRM-SC. A instituição, mediante autorização expressa da alta direção, se reserva o direito de monitorar, automaticamente, a estação de trabalho, o tráfego efetuado através das redes de comunicação, incluindo o acesso à Internet e o uso do Correio Eletrônico.

Recomendação nº 2.1: Recomenda-se ao Setor de TI, em conjunto com a Controladoria Interna, elaborar políticas e normas de TI no CRM-SC que defina as diretrizes para a Segurança da Informação.

Prazo: Dezembro/2023

Recomendação nº 2.2: Recomenda-se ao Setor de TI divulgar estas Políticas e Normas para todos os funcionários da instituição e obedecidas por todos que utilizam os recursos de arquivamento, de disponibilidade, de consultas às informações disponibilizadas e armazenadas pelo Setor de TI, sendo de responsabilidade de cada um o seu cumprimento.

Prazo: Dezembro/2023

Achado nº 03: Não atendimento do fluxo do processo de chamados da TI pelos setores do CRM-SC.

Constatou-se, através de entrevista com os gestores e de observação das atividades do Setor de TI, que os servidores do CRM-SC não estão realizando os chamados de TI pelo sistema, mas sim diretamente para os responsáveis do Setor, prejudicando as demais atividades.

O Setor de TI tem competência para, através de chamados realizados no sistema, efetuar a manutenção preventiva e corretiva dos equipamentos de informática da instituição e prestar atendimento ao usuário, assegurando o perfeito funcionamento dos equipamentos, visando garantir o controle e segurança das informações e de uso dos sistemas informatizados do CRM-SC.

Dessa forma, o mesmo deverá se responsabilizar em atender aos pedidos realizados diretamente no sistema, o qual deverá estabelecer prioridades de chamados, através de uma abordagem equilibrada.

Cada área deverá levantar as necessidades e fazer o pedido no sistema IT Manager. Enquanto o Setor de TI é responsável por analisar o pedido e manter o funcionamento da infraestrutura

Recomendação nº 3.1: Recomenda-se ao Setor de TI estabelecer normas para a realização do chamado no sistema IT Manager, determinando datas e prazos a serem atendidos, para que a área não seja prejudicada com a sobrecarga de atividades e atribuições.

Manter uma comunicação clara com as partes interessadas e ter um processo bem documentado ajuda a garantir que as prioridades sejam atribuídas de maneira justa e eficaz.

Prazo: Setembro/2023

Recomendação nº 3.2: Recomenda-se ao Setor de TI solicitar à desenvolvedora do sistema que realize aprimoramentos na ferramenta, com o intuito de que o próprio sistema, através de uma abordagem equilibrada, possa definir as prioridades, considerando tanto as necessidades técnicas quanto as operacionais e estratégicas da organização.

Prazo: Setembro/2023

Achado nº 04: O sistema IT Manager não emite relatórios gerenciais legíveis dos chamados solicitados.

Um relatório de chamados de TI é uma ferramenta essencial para acompanhar, analisar e otimizar a gestão das solicitações e problemas de tecnologia da informação em uma organização.

Com a finalidade de melhorar a tomada de decisão, os sistemas utilizados pelo CRM-SC, responsáveis por processar todos os dados, devem transformar informações úteis em informações hábeis para serem aproveitadas por todos da gestão para a tomada de decisão.

O sistema IT Manager não gera relatórios integrados, que facilitam o acesso à informação como um todo em busca de melhorar os resultados. O objetivo principal é

garantir que as informações contidas no relatório sejam claras, precisas e úteis para a tomada de decisões e aprimoramento contínuo dos processos de suporte de TI.

Recomendação nº 4.1: Recomenda-se ao Setor TI que encaminhe uma solicitação de desenvolvimento da ferramenta que gera os relatórios no sistema, contendo, no mínimo, as seguintes informações:

1. **Identificação do Chamado:**
    - Número de referência única para o chamado.
    - Data e hora de abertura do chamado.
    - Nome do solicitante (usuário).
2. **Categoria e Prioridade:**
    - Categoria do chamado (por exemplo, hardware, software, rede, etc.).
    - Nível de prioridade atribuído ao chamado (alta, média, baixa).
3. **Descrição do Problema:**
    - Descrição detalhada do problema relatado pelo usuário.
    - Informações adicionais relevantes, como mensagens de erro, comportamentos estranhos etc.
4. **Ações Tomadas:**
    - Descrição das ações realizadas pela equipe de suporte para resolver o problema.
    - Atualizações de status ao longo do processo de resolução.
5. **Tempo de Resposta:**
    - Tempo decorrido desde a abertura do chamado até o primeiro contato ou resposta da equipe de suporte.
6. **Tempo de Solução:**
    - Tempo total necessário para resolver o problema e fechar o chamado.
    - Pode ser dividido em várias etapas, como tempo de diagnóstico, tempo de implementação da solução, etc.
7. **Responsáveis:**
    - Nomes dos membros da equipe de suporte responsáveis pelo chamado.
    - Atribuição de tarefas específicas a cada membro.
8. **Solução Aplicada:**
    - Detalhes sobre a solução ou correção aplicada ao problema.
    - Passos específicos seguidos para resolver o problema.

9. **Feedback do Usuário:**
    - Qualquer feedback fornecido pelo usuário após a resolução do problema.
    - Avaliação da qualidade do suporte prestado.
10. **Observações e Notas:**
    - Quaisquer observações adicionais ou informações relevantes relacionadas ao chamado.
    - Sugestões para melhorias futuras ou medidas preventivas.
11. **Status Final:**
    - Indicação se o chamado foi resolvido com sucesso, encaminhado para níveis superiores ou se requer mais acompanhamento.
12. **Métricas e Indicadores:**
    - Dados estatísticos sobre o desempenho da equipe de suporte, como tempo médio de resposta, tempo médio de solução, número de chamados abertos/fechados, etc.
13. **Tendências e Análises:**
    - Análise de padrões recorrentes nos tipos de chamados e problemas relatados.
    - Identificação de áreas que exigem melhorias ou treinamento adicional.

Prazo: Novembro/2023

Recomendação nº 4.2: Recomenda-se ao Setor de TI que institua controles internos quanto à análise dos chamados realizados para avaliar a necessidade de personalizar as informações, conforme as necessidades da organização para obter insights relevantes e direcionar melhorias nos processos de suporte de TI.

Prazo: Dezembro/2023

Achado nº 05: Sistemas da GBR (PF e PJ) não emitem relatórios com indicadores de disponibilidade.

Os indicadores de disponibilidade são métricas essenciais no gerenciamento de serviços de TI e infraestrutura tecnológica. Eles fornecem informações cruciais sobre a capacidade de um sistema, serviço ou recurso de estar disponível e acessível para os usuários quando necessário. Esses indicadores ajudam as equipes de TI a avaliar o desempenho, a qualidade do serviço e a eficácia das operações.

Os sistemas da GBR, empresa contrata para desenvolver os sistemas utilizados pelo CRM-SC, não fornecem uma maneira de quantificar a qualidade do serviço prestado e determinar se ele atende aos níveis de serviço acordados com o CRM-SC, bem como não permitem identificar padrões de indisponibilidade recorrentes ou tendências que

podem indicar a necessidade de ajustes na infraestrutura, manutenção preventiva ou melhorias nos processos.

Constatou-se, através de entrevistas com os responsáveis pelos setores de Pessoa Física e de Pessoa Jurídica, que os sistemas possuem diversas falhas, ocasionando o retrabalho e a lentidão de alguns processos.

Os indicadores de disponibilidade podem ajudar a identificar componentes ou sistemas específicos que apresentam maior risco de falha. Isso permite que as equipes de TI priorizem esforços de manutenção e mitigação de riscos.

Recomendação nº 5.1: Recomenda-se ao Setor de TI solicitar à empresa GBR disponibilizar a opção de emitir relatórios contendo indicadores de disponibilidade, como por exemplo: o Tempo de Atividade (Uptime), o Tempo de Inatividade (Downtime), a Taxa de Disponibilidade (Availability Rate), entre outros. Essas métricas são fundamentais para manter a confiabilidade dos serviços de TI e garantir que as necessidades dos usuários e das operações de negócios sejam atendidas de forma eficaz.

Prazo: Setembro/2023

Recomendação nº 5.2: Recomenda-se ao Setor de TI implementar rotinas de controle para realizar a análise de indicadores de disponibilidade, visto que se trata de uma atividade contínua e vital para garantir que a infraestrutura de TI esteja operando de maneira eficiente e confiável.

A utilização de indicadores de disponibilidade na avaliação de fornecedores ajuda a garantir que os parceiros atendam às expectativas e garantam a continuidade e qualidade dos serviços prestados.

Prazo: Outubro/2023

Achado nº 06: Estagiários possuem acesso aos processos sigilosos.

Em geral, o acesso a processos sigilosos deve ser restrito a pessoas autorizadas e com a necessidade de acesso legítima. No caso de estagiários, o acesso a processos sigilosos deve ser tratado com cautela e seguindo as políticas de segurança e privacidade da organização.

Constatou-se que estagiários da TI e do PEP possuem acesso a alguns processos sigilosos no SGED.

A gestão de informações confidenciais é uma preocupação importante em muitos ambientes de trabalho, e isso inclui estagiários.

Recomendação nº 6.1: Recomenda-se ao Setor de TI comunicar aos Supervisores que solicitem somente o acesso que seja compatível com as atividades dos estagiários, não permitindo o acesso aos processos sigilosos do órgão.

Prazo: Setembro/2023

Recomendação nº 6.2: Recomenda-se ao Setor de TI implementar rotinas de controle para que os estagiários tenham acesso limitado a processos sigilosos e informações

sensíveis que sejam estritamente necessários para suas atribuições e sob a supervisão apropriada.

Prazo: Outubro/2023

Achado nº 07: A sala em que está localizado o data center está constantemente aberta, inclusive em momentos em que não há servidores no ambiente.

Não ter um local adequado para o data center pode acarretar uma série de riscos e problemas significativos. O data center é a espinha dorsal da infraestrutura de tecnologia de uma organização, e sua localização inadequada pode resultar em vulnerabilidades que afetam a segurança, disponibilidade e desempenho dos sistemas e serviços.

Para evitar esses perigos, é fundamental planejar, projetar e manter um data center em um local apropriado, levando em consideração a segurança física. Um local inadequado pode não oferecer proteção adequada contra roubos, vandalismos e acesso não autorizado. Isso pode resultar na perda de equipamentos valiosos e em violações de segurança.

Recomendação nº 07: Recomenda-se ao Setor de TI que mantenha um controle rigoroso de acesso ao data center. Apenas pessoas autorizadas devem ter acesso físico, e isso deve ser registrado e monitorado.

Prazo: Agosto/2023

Achado nº 08: Ausência de planejamento das necessidades de educação e treinamento.

A rápida evolução das tecnologias e as mudanças no cenário empresarial tornam o investimento em desenvolvimento de habilidades e conhecimentos uma parte essencial para o sucesso da equipe de TI e para o suporte eficaz às operações da organização.

Um planejamento de capacitação no setor de TI é essencial para manter a equipe atualizada, eficiente, inovadora e pronta para enfrentar os desafios tecnológicos em constante mudança. Isso resulta em uma equipe mais competente e uma melhor contribuição para o sucesso geral da organização

Recomendação nº 08: Recomenda-se ao Setor de TI encaminhe ao Setor de Recursos Humanos um planejamento de necessidades de treinamento e capacitação ou documento semelhante que abranja todos as atividades e servidores do Setor para ser análise e inserção das despesas no orçamento e caso necessário no plano anual de aquisições/contratações, assim contemplando a periodicidade exigida pelo CFM.

Prazo: Setembro/2023

Achado nº 09: Servidores do Setor de TI atuando como gestores e fiscais de uma elevada quantidade de contratos, representando mais de 20% de todos os realizados pelo CRM-SC.

Esse excesso de responsabilidades tem causado um volume de trabalho elevado, prazos curtos e metas inatingíveis para o Setor de TI.

Segundo o § 2º do artigo 8º do Decreto nº 11.246/2022, são considerados os seguintes aspectos para designar um gestor ou fiscal de contrato:

I. a compatibilidade com as atribuições do cargo;
II. a complexidade da fiscalização;
III. o quantitativo de contratos por agente público; e
IV. a capacidade para o desempenho das atividades.

Dessa forma, nota-se que não foram atendidos os critérios dispostos nos incisos II, III e IV ao atribuir uma quantidade elevada de contratos para serem geridos e fiscalizados pelos representantes do Setor de TI.

Recomendação nº 09: Recomenda-se à Direção do CRM-SC que realize uma redistribuição dos contratos geridos pelo Setor de TI para outras áreas do Conselho, de forma a equilibrar em todos os setores o quantitativo de atribuições referentes à gestão de contratos.

Destaca-se que, caso necessário, poderá ocorrer o desenvolvimento de competências de agentes públicos para fins de fiscalização e de gestão contratual, desde que seja demonstrado no estudo técnico preliminar.

Por fim, cumpre observar que, conforme o Decreto nº 11.246/2022, o encargo de agente de contratação, de integrante de equipe de apoio, de integrante de comissão de contratação, de gestor ou de fiscal de contratos não poderá ser recusado pelo agente público, desde que observados os critérios dispostos na referida normativa legal.

Prazo: Outubro/2023

Achado nº 10: Ausência de processos claros para identificação, resposta e resolução de incidentes de segurança, minimizando o impacto de potenciais violações.

Gerir incidentes de segurança de TI é um processo crucial para identificar, responder e mitigar as ameaças à segurança cibernética que uma organização pode enfrentar. A gestão eficaz de incidentes ajuda a minimizar danos, proteger os ativos de TI e manter a continuidade das operações.

Atualmente, o CRM-SC não possui qualquer procedimento visando a prevenção e/ou mitigação e erradicação de qualquer evento ou ocorrência que envolva a violação, comprometimento, ameaça ou exposição de sistemas de informação, redes, dados ou recursos de tecnologia da informação do órgão.

Recomendação nº 10: Recomenda-se ao Setor de TI elaborar um Plano de Respostas a Incidentes que descreva os procedimentos a serem adotados em caso de incidente de segurança. Todos os passos a serem tomados deverão ser especificados, desde a detecção até a resolução e recuperação.

A equipe de resposta a incidentes deverá ser treinada regularmente e realizar exercícios de simulação para garantir que todos saibam como agir durante um incidente real.

Prazo: Fevereiro/2024

V. CONCLUSÃO

De maneira geral, o presente trabalho constatou que a gestão do Setor de Tecnologia da Informação possui um conjunto de iniciativas e procedimentos internos que desencadeiam de forma orientada as atividades operacionais.

A auditoria revelou aspectos positivos que indicam a eficácia, a segurança e a conformidade dos sistemas, processos e práticas de TI. Aqui estão alguns aspectos positivos detectados na auditoria:

- **Backup e recuperação de dados:** Planos de backup e recuperação bem definidos que garantem a disponibilidade e a integridade dos dados mesmo em caso de falhas;
- **Gestão de ativos de TI:** Controle e gerenciamento eficazes de ativos de TI, incluindo hardware e software, para otimizar os investimentos e garantir a conformidade;
- **Segurança de rede:** Implementação de medidas de segurança de rede, como firewalls, detecção de intrusões e segmentação de rede, para proteger contra ameaças cibernéticas;
- **Atualizações de software:** Atualização regular de sistemas operacionais e aplicativos, garantindo que as últimas correções de segurança estejam em vigor;
- **Termo de responsabilidade pelo uso de recursos de tecnologia da informação**: Atualização regular do termo de responsabilidade pelo uso dos recursos de tecnologia da informação. O Setor de Recursos Humanos tem realizado o procedimento interno de solicitar a assinatura e, consequentemente, a concordância com os termos dispostos no referido documento. Esse documento prioriza tornar os processos mais cristalinos e objetivos, reforçando direitos e deveres.

No entanto, há pontos de melhorias que devem ser considerados.

O Setor demonstrou uma falta de visão estratégica, visto que os riscos não são gerenciados e há uma falta de direção clara e de visão de objetivos a longo prazo. As atividades operacionais não contribuem para metas maiores que poderá levar a uma falta de alinhamento entre todos os setores da organização. Aqui estão alguns aspectos negativos detectados na auditoria:

- **Falta de Políticas e Procedimentos:** Não há políticas e procedimentos documentados para segurança da informação, gerenciamento de riscos e outras áreas críticas;
- **Gerenciamento de riscos inadequado:** Uma abordagem reativa para identificar, avaliar e mitigar riscos de segurança e operacionais em TI;

- **Falta de Planejamento de Continuidade de Negócios:** Ausência de planos e procedimentos para lidar com interrupções e desastres que podem afetar a continuidade das operações;
- **Disponibilidade e desempenho:** Não há garantia de que sistemas críticos estejam disponíveis e funcionando de maneira eficiente para atender às necessidades da organização;
- **Controles de acesso inadequados:** A auditoria revelou que os controles de acesso estão implementados de maneira inapropriada.

A informação é um recurso estratégico, que exige cuidados especiais nos procedimentos de aquisição, de manipulação e de armazenamento. Outro ponto que exige atenção é o incremento da interconectividade, que induz maior vulnerabilidade a ameaças externas.

É importante destacar que os responsáveis pelo Setor demonstraram disponibilidade e proatividade em analisar as situações requeridas por esta Controladoria Interna, assim como contribuíram para elucidar eventuais dúvidas que surgiram durante a auditoria.

De fato, o gestor demonstrou uma preocupação no sentido de implementar um sistema de controle interno eficaz e que possa diminuir os riscos relativos ao armazenamento das informações e atualização de dados.

Com base nas considerações apresentadas neste Relatório, encaminha-se para o Setor de Tecnologia da Informação para ciência e providências.