NATUREZA DA AUDITORIA	:	CONFORMIDADE
PERÍODO DE ABRANGÊNCIA	:	01/12/2017 A 31/12/2018
UNIDADE	:	DIRTI
CÓDIGO UG	:	158132
RESPONSÁVEL	:	WILIAM RICARDO CORREIRA DIAS
CIDADE	:	CAMPO GRANDE
RELATÓRIO Nº	:	011/2017 ï AUDIT/IFMS

RELATÓRIO DE AUDITORIA INTERNA

1. INTRODUÇÃO

Em cumprimento à Ordem de Serviço 011/2017 ï AUDIT e em estrita observância ao Plano Anual de Atividades da Auditoria Interna ï PAINT 2017 do IFMS, item 18, Segurança da Informação, apresentamos os resultados dos exames realizados no período de 01 de dezembro de 2017 a 21 de dezembro de 2018.

Este trabalho buscou avaliar a estrutura dos controles internos quanto a Segurança da Informação no IFMS, considerando os normativos internos e também a conformidade com legislação que rege a matéria.

Neste contexto, importa registrar que a unidade responsável é a Diretoria de Tecnologia da Informação ï DIRTI/IFMS.

Depois de elaborada a fase de Planejamento de Auditoria, foi encaminhada à DIRTI a comunicação da realização do trabalho através do Memorando nº 195/2017/AUDIT, de 1º/12/2017, solicitando ainda a designação de uma pessoa representante daquela unidade para servir de contato e prestar esclarecimentos necessários à equipe de auditoria. Em resposta ao memorando a DIRTI encaminhou o memorando 169/2017 - DIRTI/RTRIA/IFMS, de 06/12/2017.

Com vistas a subsidiar o desenvolvimento da ação de auditoria, foi enviado a Solicitação de Auditoria nº 2017011-001/AUDIT, de 06/12/2017.

Em atendimento às Solicitações de Auditoria nº 2017011-001/AUDIT e 2017011-002/AUDIT, a DIRTI encaminhou as respostas via processo SUAP Processo 23347.010428.2018-82.

Após o término dos exames realizados, os achados de auditoria foram enviados à DIRTI por meio da Solicitação de Auditoria nº 2017011-003/AUDIT, de 21/12/2017.

A presente ação de auditoria teve que ser interrompida por excesso de atribuições e considerando que estava sendo realizada por apenas um Auditor. Retomado os trabalhos durante o mês de dezembro de 2018, em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal.

Nenhuma restrição foi imposta à realização do trabalho.

2. ESCOPO

Verificar as diretivas e controles de segurança da informação.

3. TÉCNICA E PROCEDIMENTOS DE AUDITORIA

Os procedimentos de auditoria adotados foram Testes de Observância, que têm por finalidade atestar a segurança dos controles internos estabelecidos quanto ao seu efetivo funcionamento e aderência às normas em vigor.

Foram utilizadas as seguintes técnicas de auditoria: Análise Documental, Indagação Oral e Escrita (Solicitações de Auditoria).

4. RESULTADO DOS EXAMES

Como consequência da análise dos processos, além dos informes já relatados, foram detectadas impropriedades que resultaram nas seguintes constatações.

<u>Constatação 001</u>: Política de Segurança da Informação e Comunicações ï POSIC desatualizada.

Descrição Sumária: A Política de Segurança da Informação e Comunicações ï POSIC, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul ï IFMS, foi instituída por meio do Regulamento nº 002, de 7 de fevereiro de 2011.

Causas: Ausência de controle administrativo

Fato: De acordo com o item 8, da Norma Complementar nº 03/IN01/DSIC/GSIPR, que trata da atualização da POSIC, identificamos a ausência de atualização da referida política.

> ***ñ**8 ATUALIZAÇÃO DA POSIC*
>
> *Todos os instrumentos normativos gerados a partir da POSIC, incluindo a própria POSIC, devem ser*

> *revisados sempre que se fizer necessário, não excedendo o período máximo de 03 (três) anos.***ò**

Manifestação do Gestor: ñ*Solicitamos que seja providenciada a atualização da Política de Segurança da Informação e Comunicações* **ï** *POSIC, segundo o pedido do item 1 da Solicitação de Auditoria, visto que a atual é de 2011***ò***;*

Análise da Auditoria Interna: Diante da manifestação, mantém-se o teor da constatação.

Recomendação 001: Providenciar à atualização da Política de Segurança da Informação e Comunicações ï POSIC, do Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso do Sul ï IFMS.

<u>Constatação 002</u>: Ausência de nomeação do Gestor de Segurança da Informação e Comunicações.

Descrição Sumária: Ausência de designação formal do Gestor de Segurança da Informação e Comunicações.

Causas: Ausência de controle administrativo

Fato: De acordo com o inciso IV, art. 5º, da Instrução Normativa GSI nº 01/2008, que disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, identificamos a ausência da nomeação do Gestor de Segurança da Informação e Comunicações.

> **ñ***Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:*
>
> *IV - nomear Gestor de Segurança da Informação e Comunicações;*

Manifestação do Gestor: Solicitamos ainda que seja feita a nomeação formal do Gestor de Segurança da Informação e Comunicações, segundo o pedido do item 2 da Solicitação de Auditoria;

Análise da Auditoria Interna: Diante da manifestação, mantém-se o teor da constatação.

Recomendação 001: Providenciar a designação formal do Gestor de Segurança da Informação e Comunicações.

<u>Constatação 003</u>: Ausência da instituição de equipe de tratamento e resposta a incidentes em redes computacionais.

Descrição Sumária: Ausência da instituição de equipe de tratamento e resposta a incidentes em redes computacionais.

Causas: Ausência de controle administrativo

Fato: De acordo com o inciso V, art. 5º, da Instrução Normativa GSI nº 01/2008, que disciplina a Gestão da Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, identificamos a ausência de instituição de equipe de tratamento e resposta a incidentes em redes computacionais.

> ***ñ****Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:*
>
> *V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;*

Manifestação do Gestor: ñ*O item 3 da Solicitação de Auditoria aponta a ausência da instituição de equipe de tratamento e resposta a incidentes em redes computacionais. Solicitamos que seja adicionado ao novo POSIC os nomes dos membros desta equipe como sendo os seguintes servidores lotados na Coordenação de Infraestrutura, Redes e Telecomunicações - COIRT:*

- *Helder Coelho Silva;*
- *Marcio Bambil Imai;*
- *Matheus Jardim Guerreiro da Silva;*
- *Rogério Leite e*
- *Suellen Suely da Rosa Figueiredo**ò**.*

Análise da Auditoria Interna: Diante da manifestação, mantém-se o teor da constatação.

Recomendação 001: Providenciar a designação formal da equipe de tratamento e resposta a incidentes em redes computacionais.

6. CONCLUSÃO DA EQUIPE DE AUDITORIA:

Terminados os trabalhos da equipe de auditoria, chega-se à conclusão de que a necessidade de aprimorar o controle administrativo no que tange a segurança da informação.

Contudo, destaca-se que, na análise feita acerca da segurança da informação, a necessidade de atualização da Política de Segurança da Informação e Comunicações, designação formal do Gestor de Segurança da Informação e Comunicações e Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

A fim de melhorar os controles internos, as constatações mereceram recomendações por parte desta auditoria interna, visando medidas corretivas a serem acompanhadas posteriormente. Destaque-se que as recomendações serão objeto de futuro monitoramento no PPP ï Plano de Providência Permanente, para verificar se foram adotadas, bem como se as fragilidades foram corrigidas e o controle aprimorado.

Salientamos que esta ação não tem a intenção de esgotar as possibilidades de inconsistências que podem ser observadas, mas sim, servir como orientação para as boas práticas da Administração Pública.

É importante ressaltar que as ações da Auditoria Interna devem ser sempre entendidas como atividade de assessoramento à Administração, de caráter essencialmente preventivo, destinada a agregar valor e a melhorar as operações da entidade, assistindo-a na consecução de seus objetivos mediante uma abordagem sistemática e disciplinada, fortalecendo a gestão e racionalizando as ações de Controle Interno.

Campo Grande, 21 de dezembro de 2018.

Luis Fernando Davanso Corte
Auditor-Chefe
(Port. IFMS nº 574/2014)
AUDIT/IFMS