# RELATÓRIO DE AUDITORIA INTERNA N° 04/2018

## ÁREA: TECNOLOGIA DA INFORMAÇÃO

## SUTIC

SERVIÇO PÚBLICO FEDERAL
*MINISTÉRIO DA EDUCAÇÃO*
**UNIVERSIDADE FEDERAL RURAL DO SEMI-ÁRIDO**
**UNIDADE DE AUDITORIA INTERNA**

# RELATÓRIO DE AUDITORIA INTERNA Nº 04/2018

**Dirigentes**

Magnífico Reitor Prof. José Arimatea de Matos

Nichollas Rennah Adelino de Almeida (SUTIC).

**Área:**

Superintendência de Tecnologia da Informação

**Origem da Demanda:** PAINT/2018

## A. Introdução

A Superintendência de Tecnologia da Informação e Comunicação (SUTIC) e tem por objetivo, desenvolver as atividades de gestão da Tecnologia de Informação e Comunicação da instituição. Cabe a SUTIC o planejamento, a coordenação, a organização, em nível central, da tecnologia da informação e comunicação a fim de alinhar os objetivos, ações e metas às estratégias do Plano de Desenvolvimento Institucional (PDI). Dentre as atribuições da SUTIC, podemos destacar:

- Planejar e viabilizar o desenvolvimento dos projetos relacionados ao PDTI;

- Identificar as necessidades da instituição quanto a Tecnologia da Informação e Comunicação e planejar o desenvolvimento de projetos para o atendimento dessas necessidades;
- Propor políticas de Tecnologia da Informação e Comunicação e de Segurança da Informação e Comunicação para a instituição;
- Avaliar os riscos nos projetos de Tecnologia da Informação e Comunicação;
- Gerenciar os investimentos de Tecnologia da Informação e Comunicação e propor recursos para ações de Segurança da Informação e Comunicação;
- Acompanhar as investigações e avaliações dos danos decorrentes de quebras de segurança da informação no âmbito da instituição.

Por ser uma atividade estratégica e essencial à organização, de alta relevância, que nunca foi auditada em anos e trabalhos anteriores, a área de TI passou a incorporar a Matriz de Risco dos trabalhos de Auditoria, inseridos no PAINT 2018, aprovado pelo Conselho de Administração da Instituição e pela Controladoria Geral da União – CGU.

## B. Objetivo

A presente atividade de auditoria teve por objetivo aferir e avaliar as atuais condições dos controles administrativos internos na área da Tecnologia da Informação – **em especial os controles relacionados Governança e à Segurança da Informação.** Os trabalhos foram realizados durante o período de outubro a dezembro de 2018 pela Auditoria Interna UFERSA. Foram utilizados diversos procedimentos e técnicas de auditoria para a consecução dos objetivos pretendidos, em especial: testes de observância e testes substantivos, englobando a conferência de documentos e dados extraídos dos sistemas operacionais de informações em uso pela unidade.

Em suma, o presente trabalho buscou avaliar os procedimentos, fluxos, mecanismos e ferramentas de controle utilizados e em efetivo funcionamento no âmbito da Tecnologia da Informação, em especial da Segurança da Informação na UFERSA.

## C. Da Metodologia

Encaminhamento de Solicitação Auditoria ao departamento envolvido; análise do material e seleção de amostras; registro das constatações e recomendações; elaboração do relatório final que ficará disponível para consulta pública no endereço eletrônico da AUDINT UFERSA no portal da Instituição.

## D. Período de Realização

a) Planejamento: 01/10 a 11/10/2018

b) Execução: 15/10 a 15/12/2018

c) Encerramento – Análise dos Papéis de Trabalho e Relatórios – 15/12 a 20/12/2018

## E. Equipe e Horas/Atividades

| AUDITORES | ATIVIDADE | HORA/ATIVIDADE |
|---|---|---|
| Marília de Lima Pinheiro Gadêlha Melo | Coordenação de Campo / Planejamento / Análise de Processos /Relatório | 200h |

## 1. CONSIDERAÇÕES INICIAIS

Os trabalhos foram realizados dentro dos prazos previstos, sendo que nenhuma restrição foi imposta aos nossos trabalhos. Abaixo seguem as informações e constatações verificadas no decorrer dos trabalhos de auditoria, bem como as respectivas recomendações desta Unidade de Auditoria Interna, para a avaliação, conhecimento e providências que a gestão porventura julgar oportunas, convenientes e cabíveis.

## 2. RESULTADOS DOS TRABALHOS

Inicialmente cumpre observar que o Relatório mencionará achados de auditoria com recomendações, mas também informações que não gerem recomendações, mas que são consideradas relevantes e passíveis de futuro monitoramento.

**INFORMAÇÃO**: Realização de backup e Política de cópia de segurança.

Foi verificado que existe a rotina de realização de cópias de segurança dos dados armazenados conforme resposta da SUTIC a nossa Solicitação, in verbis:

1. *Trata-se de uma prática realizada pela SUTIC em diversos cenários. Do ponto de vista de dados de sistemas e dos próprios sistemas, são realizados backups diários, durante a madrugada. Estas cópias são replicadas e armazenadas no datacenter e em um segundo ambiente. Planeja-se pelo menos mais dois pontos adicionais. A periodicidade diária é compatível com o fluxo e a rotina de dados gerada pela instituição e é compatível com os equipamentos que possuímos para realizar estas tarefas. Além dos dados propriamente ditos, também temos: links redundantes, aplicações em execução em mais de um servidor, infraestrutura de rede descentralizados (a parada de um campi não implica na parada de outro), redundância dos dispositivos de segurança (firewall) e replicação dos mesmos nos campi. Para a Gestão da Continuidade, o backup da infraestrutura é de grande importância.*

Nesse viés, embora haja o referido backup, em memorando eletrônico anterior nº 32/2018-SUTIC o superintendente afirmou que não foram instituídas política de cópia de segurança, a qual será apresentada até junho de 2019 perante o Comitê de governança digital da UFERSA. Nesse sentido, o serviço ainda poderá gerar riscos em razão da ausência de formalização e padronização dos processos quanto a cópias de segurança.

Desta feita, deixa-se de expedir recomendação, diante do compromisso da aprovação da referida política ainda no primeiro semestre do exercício de 2019, o que será objeto de monitoramento pela AUDINT.

**CONSTATAÇÃO 1: Ausência de política de gestão de riscos de TI.**

De acordo com informações fornecidas no memorando eletrônico nº 32/2018- SUTIC inexiste a política de gestão de riscos em TI e se pretende aguardar o amadurecimento da Gestão de Riscos como um todo na instituição para integrar essa medida de gestão com as demais áreas da instituição.

**Recomendação 1.1:**

Elaborar um procedimento formalizado de gerenciamento de riscos de TI, de acordo com o PDTI e executá-lo conforme as necessidades técnicas da área e institucionais, visando a mitigação e redução dos riscos residuais e inerentes à área de TI.

**CONSTATAÇÃO 2: Inexistência de Comitê de Gestão de TI.**

Foi constatado que em que pese existir a Política de segurança da informação e gestão de continuidade de negócio relativa aos serviços de TI, não se detectou uma execução eficaz dessa política, não foi criado e implementado no UFERSA um Comitê de Gestão de TI, que contemple a segurança em tecnologia da informação.

Além disso quase não há informações públicas acessíveis quanto a atividade na plataforma de governança digital da UFERSA, o que se confirmou com dados informados acerca da ausência do comitê formal de gestão de TI, além de não haver diretrizes para avaliação da governança e gestão de TI, como informado pela SUTIC no memorando eletrônico nº 32/2018.

**Recomendação 2.1:**

Nesse prisma, impende sejam tornadas concretas e efetivas as medidas já formalizadas quanto a governança e gestão de riscos em TI, bem como formalizar e concretizar na prática outras acima destacadas como ausentes.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Dessa forma, recomendamos a criação imediata do Comitê de Gestão TI, que contemple a área de segurança em tecnologia da informação, bem como as áreas de segurança física, patrimonial, etc, constituído por uma equipe multidisciplinar de servidores. E que se efetive a política se segurança da informação e gestão de continuidade de negócio relativos aos serviços/processos de TI.

**CONSTATAÇÃO 3**: **Falta de atendimento a necessidades do PDTI vigente.**

Em que pese ainda haver prazo para conclusão de metas, verificou-se que algumas necessidades constantes no PDTI atual ainda não foram totalmente cumpridas e atendidas, mas muitas também foram alcançadas.

Não há documento público que mensure até aqui o que já foi alcançado de metas e o que está pendente, o que mitiga nossa análise, pelo que se faz necessário que se formalize o monitoramento do PDTI para que se mensure seu sucesso e as metas que serão repactuadas, com as justificativas formais.

**Recomendação 3.1:**

Iniciar as tratativas e trabalhos para atendimento das necessidades que ainda não possuem indicação de atingimento de meta, com brevidade e celeridade, e concluir os processos para atendimento daquelas necessidades que já foram iniciadas e por algum motivo não finalizadas.

## 3. REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2006. Sistemas de gestão de segurança da informação. ABNT NBR ISO/IEC 27002:2005. Código de prática para a gestão da segurança da informação.
Decreto nº 3.505/2000. Institui Política de Segurança da Informação na Administração Federal.
COBIT 4.1.
Manual de Boas Práticas em Segurança da Informação do Tribunal de Contas da União – 2012.
PDTI UFERSA 2015-2019.

## 4. CONSIDERAÇÕES FINAIS

Após a finalização dos trabalhos de análises em campo, na área da Tecnologia da Informação – Segurança da Informação, esta Unidade de Auditoria Interna/ UFERSA, encaminha o presente relatório para a Secretaria dos órgãos Colegiados-SOC e SUTIC, indicando as principais inconsistências encontradas.

A Unidade de Auditoria Interna irá acompanhar e monitorar as recomendações propostas durante o ano de 2019 visando ampliar e melhorar os controles administrativos internos na área da Tecnologia da Informação.

Em geral, os controles internos ora auditados merecem uma atenção especial por parte da equipe diretiva da SUTIC, principalmente os relacionados à segurança da informação que carecem de uma política efetivamente aprovada e implantada.

Independente das recomendações que serão objeto de monitoramento pela AUDINT, cabe à equipe de gestores a análise de cada item destacado neste Relatório, sendo que o acatamento das propostas contidas neste Relatório constitui interesse exclusivo dos gestores.

Por fim, a equipe de auditores, abaixo identificada, agradece a SUTIC pela disponibilidade das informações e materiais requisitados e acolhida da equipe, e se coloca à disposição para elucidar quaisquer inconsistências ou inconformidades relatadas, visando, sobretudo, o fortalecimento dos controles internos do UFERSA.

Mossoró, 20/12/2018.

**Marília de Lima Pinheiro**
**Gadêlha Melo**
**Chefe de Auditoria UFERSA**
**Matrícula SIAPE: 1895233**

*OBS: O documento original encontra-se assinado.