RELATÓRIO DE AUDITORIA **9/2015/AUDIN**

Dirigente: Magnífico Reitor Mauro Augusto Burkert Del Pino
Unidade Auditada: Coordenação de Tecnologia da Informação
Gestor: Amanda Argou
Período da Auditoria: outubro de 2015 a fevereiro de 2016
Auditora: Letícia dos Passos Pereira Dias

1. APRESENTAÇÃO

A Auditoria Interna da Universidade Federal de Pelotas, considerando as atribuições estabelecidas no Decreto nº 3.591/2000 e em atendimento à ação nº 09 – Gestão de Tecnologia da Informação, do Plano Anual das Atividades de Auditoria Interna - PAINT/2015, aprovado através do Ofício nº 2566/2015/GAB/CGU-Regional/RS/CGU-PR, apresenta o Relatório de Auditoria Interna nº 09.01/2015/AUDIN.
A presente auditoria teve início com a expedição da Ordem de Serviço nº 06/2015, seguida de reunião entre a Audin e os responsáveis pela gestão de tecnologia da informação na UFPel. A reunião teve por finalidade informar aos gestores os objetivos dos trabalhos, bem como apresentar o projeto desta auditoria.
Os trabalhos foram realizados na Unidade de Auditoria Interna da UFPel, em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal.
Nenhuma restrição foi imposta aos exames.

2. EXECUÇÃO DOS TRABALHOS

2.1. Objetivo

Avaliar a gestão de tecnologia da informação na UFPel no que tange à política de segurança da informação e ao desenvolvimento de sistemas.

2.2. Escopo

- Verificar o cumprimento das normas referentes à Segurança da Informação no âmbito da Universidade;
- Verificar se os sistemas estão sendo desenvolvidos de acordo com o Plano Diretor de Tecnologia da Informação (PDTI) e com o Plano Estratégico de Tecnologia da Informação (2013 – 2015).

2.3. Critérios

Os critérios para fundamentar as análises apresentadas neste trabalho foram, dentre outros, os preceitos constitucionais e os seguintes instrumentos normativos:

- GSI/PR – IN GSI/PR nº 01, de 13/06/2008;
- Norma Complementar nº 03/IN01/DSIC/GSIPR, de 30/09/2009;
- Norma Complementar nº 04/DSIC/GSIPR, de 14/08/2009;
- Norma Complementar nº 07/DSIC/GSIPR, de 06/05/2010;
- Documento e-PING 2014;

- Guia de Boas Práticas em Segurança da Informação – TCU;
- EGTI (2013 – 2015);
- PDTI (2012 – 2013);
- Plano Estratégico (2013 – 2015).

2.4. Metodologia
As principais técnicas utilizadas foram as de entrevista, indagação escrita, análise documental, inspeção física e aplicação de *check list*.

3. CONSTATAÇÕES

3.1. Constatação 01
Constatamos que na Universidade não há "Gestor de Segurança da Informação e Comunicações" formalmente designado.

Critérios
Art. 5º, IV da IN 01/2008 GSI/PR e item 5.3.7.2 da Norma Complementar 03/IN01/DSIC/GSIPR, de 30/09/2009, transcritos abaixo:

IN 01/2008 GSI/PR

> 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;

NC 03/IN01/DSCI/GSIPR:

> 5.3.7 **Competências e Responsabilidades**: neste item recomendam-se os seguintes procedimentos:
> 5.3.7.2 Instituir o **Gestor de Segurança da Informação e Comunicações** do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso, com as seguintes responsabilidades:
> a) Promover cultura de segurança da informação e comunicações;
> b) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
> c) Propor recursos necessários às ações de segurança da informação e comunicações;
> d) Coordenar o Comitê de Segurança da Informação e Comunicações e a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;
> e) Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
> f) Manter contato permanente e estreito com o Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à segurança da informação e comunicações;
> g) Propor Normas e procedimentos relativos à segurança da informação e comunicações no âmbito do órgão ou entidade da APF

Evidências
Em resposta à S.A 09.02/AUDIN/2015 o gestor informou que *"A Instituição não possui um gestor de segurança da informação e comunicações formalmente designado. Percebe-se também a falta de pessoal designado e qualificado em outros setores da Universidade exclusivamente dedicado para atuar com a gestão da segurança da informação no âmbito Institucional."*

Análise da Auditoria Interna:
Em 14 de janeiro de 2016:
Em sua resposta, o gestor admite a inexistência de gestor de segurança da informação e comunicações formalmente designado na Instituição. Assim, de acordo com as normas vigentes e considerando que a nomeação de uma pessoa com tal responsabilidade contribuirá para o aprimoramento dos controles internos atinentes à segurança da informação, emitimos a seguinte recomendação:

Recomendação nº 01:

Recomendamos que a Instituição designe formalmente um "Gestor de Segurança da Informação e Comunicações".

3.2. Constatação 02
Constatamos que não há política de segurança da informação e comunicações (POSIC) formalizada e aprovada pela autoridade máxima da UFPel.

Critérios
Art. 5º, VII da IN 01/2008 GSI/PR e item 4.4 da Norma Complementar 03/IN01/DSIC/GSIPR, de 30/09/2009, transcritos abaixo:

IN 01/2008 GSI/PR

> Art. 5º Aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:
> (...)
> VII - aprovar Política de Segurança da Informação e Comunicações e demais normas de segurança da informação e comunicações;

03/IN01/DSIC/GSIPR

> Para a institucionalização da POSIC no órgão ou entidade da APF, são recomendadas as seguintes ações:
> 6.1 Implementar a POSIC através da formalização e da aprovação por parte da autoridade máxima responsável pelo órgão ou entidade da APF, demonstrando a todos os servidores e usuários o seu comprometimento.

Evidências
Em resposta à S.A 09.02/AUDIN/2015 o gestor informou que *"Em que pesem todos os esforços empreendidos, a construção de uma POSIC é substancialmente complexa, já que, envolve questões de toda a instituição e de seus diversos setores, perpassando as competências desta Coordenação de Tecnologia da Informação. Contudo, é satisfatório neste momento, informarmos que contamos com um de nossos servidores trabalhando arduamente e outros contribuindo na revisão, da proposta de Política de Segurança da Informação e Comunicações (POSIC) que acompanha a presente resposta, aguardando a próxima reunião do Comitê de Segurança da Informação para discussão e posterior aprovação e/ou alteração da mesma."*

Análise da Auditoria Interna
Em 14 de janeiro de 2016:

Tendo em vista que as normas que determinaram a implementação de uma política de segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal foram editadas em 2008 e 2009, consideramos que já transcorreu tempo razoável para Instituição formalizá-la e aprová-la. Desta forma, esta AUDIN, como forma de contribuir para o fortalecimento dos controles internos da Universidade, emite a seguinte recomendação:

Recomendação nº 02:

Recomendamos à UFPel que formalize e aprove a sua Política de Segurança da Informação e Comunicações (POSIC).

3.3. Constatação 03

Constatamos que na minuta da POSIC, em fase de elaboração na UFPel, não foram incluídas diretrizes sobre os seguintes temas: "Tratamento da Informaçao", "Tratamento de Incidentes", " Gestão de Risco e Gestão de Continuidade", "Uso de e-mail" e "Acesso à Internet".

Critérios

Item 5.3.5 da Norma Complementar 03/IN01/DSIC/GSIPR, a seguir transcrita:

> 5.3 Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens:
> (...)
> 5.3.5 Diretrizes Gerais: neste item recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as Normas específicas vigentes no ordenamento jurídico:
> a) Tratamento da Informação;
> **b) Tratamento de Incidentes de Rede;**
> **c) Gestão de Risco;**
> **d) Gestão de Continuidade;**
> e) Auditoria e Conformidade;
> f) Controles de Acesso;
> **g) Uso de e-mail; e**
> **h) Acesso a Internet.**

Evidências

Minuta da POSIC enviada juntamente com a resposta à S.A. 09.02/2015/AUDIN.

Análise da Auditoria Interna

Em 14 de janeiro de 2016:

A Norma Complementar 03/IN01/DSIC/GSIPR estabelece diretrizes para elaboração da Política de Segurança da Informação e Comunicações (POSIC) no âmbito da Administração Pública Federal Direta e Indireta. No item 5.3.5 da referida norma são estabelecidos temas sobre os quais a POSIC deve conter diretrizes gerais. Analisando a POSIC verificamos que os temas previstos nas alíneas "b", "c", "d", "g", e "h" não foram incluídos. Assim, considerando que a POSIC da UFPel ainda está pendente de aprovação e como forma de contribuir para o fortalecimento dos controles internos, emitimos a seguinte recomendação:

Recomendação nº 03:

Recomendamos que sejam incluídas na POSIC diretrizes gerais sobre os seguintes temas: "Tratamento da Informaçao", "Tratamento de Incidentes", " Gestão de Risco" e "Gestão de Continuidade", "Uso de e-mail" e "Acesso à Internet".

3.4. Constatação 04

Constatamos que a minuta da POSIC, em fase de elaboração na UFPel, não prevê a constituição de "Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais".

Critérios

Item 5.3.7.4 da Norma Complementar 03/IN01/DSIC/GSIPR, a seguir transcrita:

> 5.3.7 Competências e Responsabilidades: neste item recomendam-se os seguintes procedimentos:
> (...)
> 5.3.7.4 Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF.

Evidências

Minuta da POSIC enviada juntamente com a resposta à S.A. 09.02/2015/AUDIN.

Análise da Auditoria Interna

Em 14 de janeiro de 2016:

A Norma Complementar 03/IN01/DSIC/GSIPR estabelece diretrizes para elaboração da Política de Segurança da Informação e Comunicações (POSIC) no âmbito da Administração Pública Federal Direta e Indireta. "A referida norma prevê que a POSIC deve instituir Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais", o que não ocorreu. Desta forma, no intuito de contribuir para o fortalecimento dos controles internos, emitimos a seguinte recomendação:

Recomendação nº 04

Recomendamos que na POSIC seja instituída "Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais" nos termos da Norma Complementar 03/IN01/DSIC/GSIPR.

3.5. Constatação 05

Constatamos que o ambiente da rede do sítio da UFPel não conta com planos de contingência implementados e atualizados, visando ao pronto restabelecimento do ambiente e dos serviços, caso seja necessário.

Critérios

Art. 25 da Res. 07/2002 do Comitê Executivo Do Governo Eletrônico/PR, abaixo transcrito:

> Art. 25. O ambiente da rede do sítio do órgão ou entidade deve contar com planos de contingência implementados e atualizados, visando ao pronto restabelecimento do ambiente e dos serviços, assim como o não comprometimento da imagem da Administração Pública Federal;

Evidências

Em resposta à S.A 09.02/AUDIN/2015 o gestor informou que *"Atualmente, a Coordenação de Tecnologia da Informação adota procedimentos para o pronto restabelecimento do ambiente, dos*

serviços e o comprometimento da imagem da Administração Pública Federal. Neste sentido, podemos citar a realização de cópias de segurança de nossos sites.
Assim, ao ser identificado o ataque ou comprometimento do site, se este for gerenciado pela unidade gestora de TI, automaticamente são adotadas as seguintes práticas:
- Coleta de dados para avaliação do incidente;
- Correção da falha;
- Restauração do ambiente.
Caso o website não esteja sob a gerência da unidade gestora de TI, o procedimento é:
- Coletar os dados para avaliação do incidente;
- Tornar o site inacessível até que a efetiva correção seja aplicada pelos responsáveis;
- Comunicar aos responsáveis;
Entretanto, ainda não possuímos um documento formal de planos de contingência implementados e atualizados."

Análise da Auditoria Interna
Em 14 de janeiro de 2016:
Em sua resposta à S.A 09.02/AUDIN/2015, o gestor informa que são adotados procedimentos para o pronto restabelecimento do ambiente e dos serviços, assim como para o não comprometimento da imagem da Instituição, porém admite que não há um plano de contingência implementado. Assim, como forma de contribuir para o aperfeiçoamento dos controles internos em matéria de Segurança da Informação, emitimos a seguinte recomendação:

Recomendação nº 05:

Recomendamos, como forma de garantir a segurança do ambiente da rede do sítio da UFPel, seja implementado Plano de Contingência nos termos do art. 25 da Resolução 07/2002 do Comitê Executivo do Governo Eletrônico/PR.

3.6. Constatação 06
Constatamos que as instalações dos ambientes de *Data Center*[1] da UFPel são inadequadas para garantir a segurança física dos ativos de informação.

Critérios
- Norma TIA 942 (*Telecommunications Infrastructure Standard for Data Center*), que consiste no padrão de telecomunicações e infraestrutura para *Data Center*.
- Norma Complementar nº 04/IN01/DSIC/GSIPR - Gestão de riscos de segurança da informação e comunicações – GRSIC
- Norma Complementar nº 07/IN01/DSIC/GSIPR - Diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações.

Evidências
Em resposta à S.A 09.02/AUDIN/2015 o gestor informou que *"Os ambientes operacionais onde se encontram os servidores de arquivos, banco de dados e infraestrutura central de rede (Data Center) são estruturados sob 4 pilares básicos: Civil (incluindo controle e monitoramento de*

[1] *Data Center* é o local onde são concentrados os equipamentos de processamento e armazenamento de dados de uma empresa ou organização.

acesso, detecção e combate a incêndio), Elétrico (incluindo distribuição e energia reserva), Climatização e Telecomunicações.

Civil: ambos não contam com segurança física adequada, faltam recursos de controle e monitoramento remoto (câmeras) de acesso, sensores (sistema de detecção e combate a incêndios). (...)
Climatização: não há redundância em refrigeração, o sistema de ar condicionado deve ser projetado para ter o funcionamento contínuo de 24x7x365, fator que é alcançado com equipamentos de precisão. Atualmente os dois Data Center estão equipados com sistemas de baixa performance, já que possuem apenas aparelhos condicionadores de ar de uso doméstico e não o que seria apropriado: os de alta precisão."

Nas fotos 1 e 2, obtidas no *Data Center* do Câmpus Capão do Leão, observamos que não há controle de entrada e saída de pessoas:

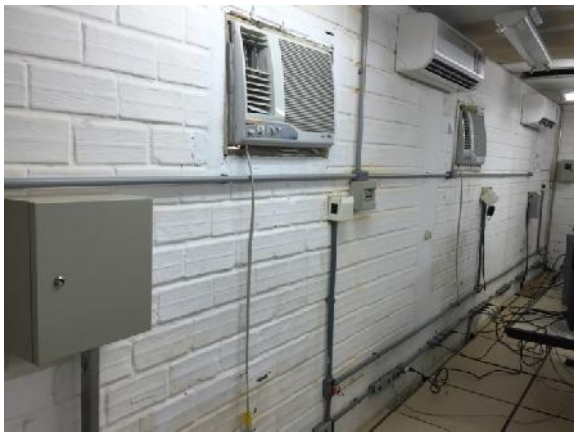
Foto1

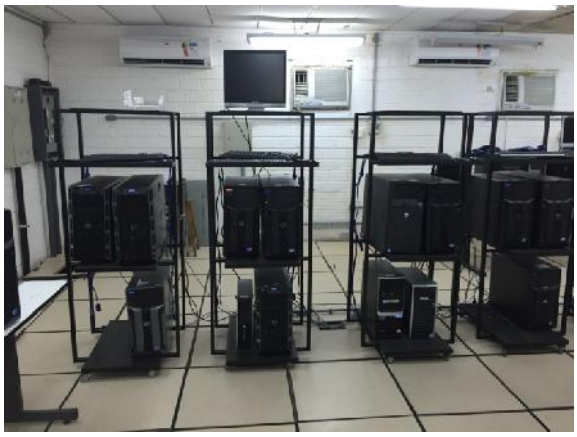
Foto 2

Na foto 3 é possível observar que o local não conta com sistema de detecção de fumaça e de atuação automática de gases inibidores de incêndio, havendo apenas alguns extintores:

Foto 3

Nas fotos 4 e 5 observamos que o local conta apenas com aparelhos de ar condicionado de uso doméstico:





Análise da Auditoria Interna
Em 14 de janeiro de 2016:
A "informação" pode ser considerada um dos ativos mais importantes e críticos dentro de qualquer organização. Informações indisponíveis, adulteradas ou sob o conhecimento de pessoas não autorizadas podem comprometer o andamento dos processos institucionais. Em vista disso, um ambiente de *Data Center* deve contar com infraestrutura adequada que garanta a segurança física dos ativos de TI.

Contudo, nos ambientes de *Data Center* da UFPel a situação encontrada é a seguinte:

- O acesso de pessoas aos ambientes operacionais não é devidamente controlado;
- Os locais não contam com mecanismos efetivos de detecção e combate a incêndios;
- As especificações para temperatura e umidade relativa do ambiente não são atendidas.

Desta forma, objetivando o aperfeiçoamento dos controles internos e primando pela segurança física dos ativos de informação, emitimos as seguintes recomendações:

Recomendação nº 6.1:

Recomendamos que sejam implementados meios de controle efetivos a fim de evitar o acesso de pessoas não autorizadas aos ambientes de *Data Center* da UFPel, tais como: câmeras com monitoramento remoto, sensores de presença, leitores biométricos e alarmes contra invasão.

Recomendação nº 6.2:

Recomendamos sejam instalados nos ambientes de *Data Center* da UFPel equipamentos adequados de detecção e combate a incêndios, tais como detectores de fumaça e sistemas de atuação automática de gases inibidores.

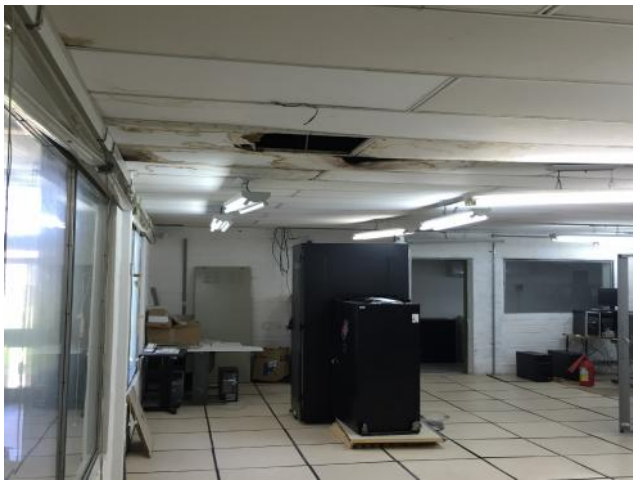
Recomendação nº 6.3:

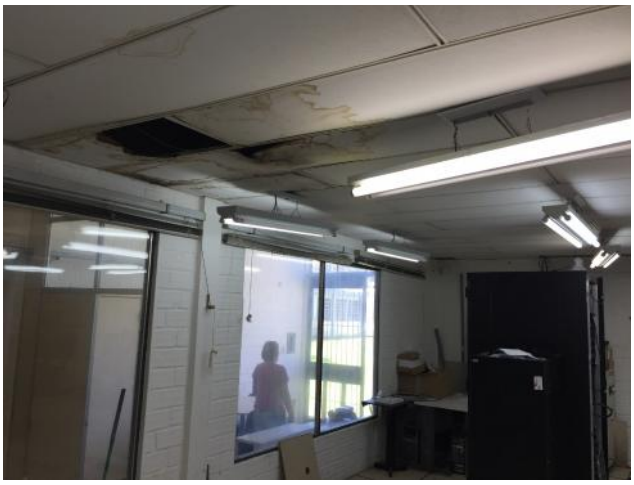
Recomendamos que nos ambientes de *Data Center* da UFPel seja instalado sistema de refrigeração que proporcione de forma contínua condições adequadas de temperatura e umidade do ar para este tipo de ambiente.

3.7. Constatação 07
Constatamos que o *Data Center* localizado no Câmpus Capão do Leão está em local no qual o teto está bastante danificado, com buracos e infiltrações de água.

Critérios
Norma ANSI/EIA/TIA 942 (*Telecommunications Infrastructure Standard for Data Center*), que consiste no padrão de telecomunicações e infraestrutura para *Data Center.*

Evidências
Nas fotos abaixo, obtidas no local onde se encontra o *Data Center* do Câmpus Capão do Leão, observamos a existência de buracos e infiltrações de água no teto:





Análise da Auditoria Interna
Em 14 de janeiro de 2016:
Nas fotos tiradas no local onde está o *Data Center* é possível observar que o teto da sala apresenta buracos e infiltrações de água. É, portanto, evidente que há risco de os equipamentos terem contato com água infiltrada e também de desabamento de parte do teto, o que pode ocasionar o comprometimento dos ativos de TI. Assim, no intuito de contribuir para o fortalecimento dos controles internos em Segurança da Informação, recomendamos o seguinte:

Recomendação nº 07:

Recomendamos que o teto da sala onde está o *Data Center* localizado no Câmpus Capão do Leão seja consertado, de modo que os buracos e as infiltrações de água sejam eliminados.

3.8. Constatação 08
Constatamos que a Instituição não adota critérios de classificação das informações de modo que possam receber tratamento diferenciado conforme grau de importância, criticidade e sensibilidade.

Critérios
TCU – Boas Práticas em Segurança da Informação, pp. 61 e 62, contendo os seguintes trechos de acórdãos:

Acórdão 465/2011 - Plenário

> "(...) em atenção ao Decreto 4.553/2002, art. 6º, § 2º, II, e art. 67, crie critérios de classificação de informações, a fim de que possam ter tratamento diferenciado conforme seu grau de importância, criticidade e sensibilidade, com observância das práticas contidas no item 7.2 da NBR ISO/IEC 27.002."

Acórdão 381/2011 - Plenário

> "(...) implemente o prescrito no art. 6º da sua Política de Segurança da Informação, criando critérios de classificação das informações, a fim de que elas possam ter tratamento diferenciado em termos de seu valor, requisitos legais, grau de sensibilidade, grau de criticidade e necessidade de compartilhamento, considerando o teor do Decreto 4.553/2002, art. 6º, § 2º, I e II, e art. 67, e observando as práticas contidas no item 7.2 da Norma Técnica – NBR – ISO/IEC 27002, item 7.2 – Classificação da informação, conforme tratado no achado 14 – Inexistência de classificação da informação – do relatório de fiscalização;

Art. 27 da Lei 12.527/2012 (Lei da transparência), a seguir transcrito:

> Art. 27. A classificação do sigilo de informações no âmbito da administração pública federal é de competência:
> I - no grau de ultrassecreto, das seguintes autoridades:
> a) Presidente da República;
> b) Vice-Presidente da República;
> c) Ministros de Estado e autoridades com as mesmas prerrogativas;
> d) Comandantes da Marinha, do Exército e da Aeronáutica; e
> e) Chefes de Missões Diplomáticas e Consulares permanentes no exterior;
> II - no grau de secreto, das autoridades referidas no inciso I, dos titulares de autarquias, fundações ou empresas públicas e sociedades de economia mista; e
> III - no grau de reservado, das autoridades referidas nos incisos I e II e das que exerçam funções de direção, comando ou chefia, nível DAS 101.5, ou superior, do Grupo-Direção e Assessoramento Superiores, ou de hierarquia equivalente, de acordo com regulamentação específica de cada órgão ou entidade, observado o disposto nesta Lei.

Itens 7.2.1 e 7.2.2 da ABNT NBR ISO/IEC 27002 (Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação):

> A.7.2.1 Recomendações para classificação (*Controle):* A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
> A.7.2.2 Rótulos e tratamento da informação (*Controle):* Um conjunto apropriado de procedimentos para rotular e tratar a informação deve ser definido e implementado de acordo com o esquema de classificação adotado pela organização.

Norma Complementar 20/IN01/DSIC/GSIPR - que estabelece diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal.

Evidências

Em resposta à S.A 09.02/AUDIN/2015 o gestor informou ***"****Importante salientar que, a Segurança das informações não está restrita apenas à área de Tecnologia da Informação e a esta Coordenação de TI, ela envolve toda a Universidade. Atualmente a instituição não estabelece critérios internos de classificação das informações, existe um indicativo de que estas questões possam ser tratadas em Norma específica derivada da POSIC."*

Análise da Auditoria Interna
Em 14 de janeiro de 2016:
Por ser a "informação" um recurso patrimonial de elevada importância para qualquer instituição, a legislação vigente exige que sejam adotados critérios para classificá-la e protegê-la em nível adequado. O TCU também traz em seu compilado de boas práticas em segurança da informação, trechos de acórdãos fazendo referência à classificação e tratamento da informação institucional. A exigência também está prevista na ABNT NBR ISO/IEC 27002 (Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação). Assim, como forma de contribuir para aprimoramento dos controles internos, emitimos a seguinte recomendação.

Recomendação nº 08:

Recomendamos sejam adotados pela UFPel critérios de classificação das informações a fim de que possam receber tratamento diferenciado conforme grau de importância, criticidade e sensibilidade.

3.9. Constatação 09
Constatamos que os servidores que são desligados da UFPel continuam possuindo acesso aos sistemas de informação que operavam em razão do trabalho.

Critério
TCU – Boas Práticas em Segurança da Informação, p. 65, contendo o seguinte trecho de acórdão:

Acórdão 782/2004 – 3ª Câmara

> 9.2.1. adote procedimentos formais de concessão e de validação periódica de senhas de usuários de sistemas informatizados, bem como de cancelamento de acesso de usuários que são desligados da unidade;

Item 8.3.3 da ABNT NBR ISO/IEC 27002 (Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação):

> 8.3.3 Os direitos de acesso de todos os funcionários, fornecedores e terceiros às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança destas atividades.

Evidências
Em resposta à S.A 09.02/AUDIN/2015 o gestor informou que *"Por outro lado, o cancelamento do acesso de usuários que são desligados da unidade depende da informação do custodiante da informação, o que gera na prática, algumas distorções nos dados institucionais ocasionadas por demora ou má alimentação dos sistemas".*

Diante do que foi relatado pelo gestor responsável pela área de Tecnologia da Informação, questionamos à Pró-Reitoria de Gestão de Pessoas (PROGEP) quais os procedimentos realizados quando ocorre o desligamento do servidor e se os setores competentes são avisados para que os acessos a sistemas e e-mails institucionais sejam bloqueados. A resposta da PROGEP foi a seguinte:

Núcleo de cadastro: *"Informamos que não adotamos procedimentos referentes a bloqueio de acessos a sistema e e-mails, na ocorrência de desligamento de servidores."*

Núcleo de Benefícios: *"No tocante às atividades desenvolvidas neste Núcleo de Benefícios, informamos que não adotamos procedimentos quanto a informação para bloqueio de acesso aos sistemas da UFPel por parte dos servidores por ocasião da aposentadoria."*

Análise da Auditoria Interna
Em 14 de janeiro de 2016:
Diante das manifestações dos setores envolvidos, resta claro que os servidores que são desligados da UFPel continuam possuindo acesso aos sistemas de informação que operavam em razão do trabalho. Tal situação contraria entendimento do TCU e normas da ABNT, gerando riscos à integridade das informações armazenadas. Assim, com o propósito de contribuir para o fortalecimento dos controles internos, emitimos a seguinte recomendação:

Recomendação nº 09:

Recomendamos sejam cancelados os acessos dos servidores desligados da UFPel aos sistemas de informação institucionais.

3.10. Constatação 10
Constatamos que não foram instituídos critérios a serem observados para definição das prioridades no que tange ao desenvolvimento de sistemas de informação na UFPel.

Critérios
PDTI/UFPel 2012-2013, no qual consta o seguinte objetivo específico: "Definir e institucionalizar os critérios de prioridade e atendimento de demandas para o desenvolvimento de sistemas de informação na UFPEL."

Evidências
Em resposta à S.A 09.02/2015/AUDIN, o gestor informou que *"Atualmente, a administração Superior da UFPel, estabeleceu as prioridades para atendimento das demandas de desenvolvimento de sistemas de informação na UFPel, contudo, não estabeleceu os critérios a serem observados.*

Em resposta à S.A 09.04/2015/AUDIN, o gestor informou que *"(...) Conforme anteriormente informado, a administração Superior da UFPel, estabeleceu as prioridades para atendimento das demandas de desenvolvimento de sistemas de informação na UFPel, contudo, não estabeleceu os critérios a serem observados.*
Assim, as prioridades são estabelecidas de acordo com o entendimento dos dirigentes da Administração Superior (Reitor, Vice-Reitora, Pró-Reitores)."

Análise da Auditoria Interna
Em 14 de janeiro de 2016:
Diante das respostas do gestor às solicitações de auditoria 09.02 e 09.04/2015/AUDIN, resta inequívoco que o objetivo "Definir e institucionalizar os critérios de prioridade e atendimento de

demandas para o desenvolvimento de sistemas de informação na UFPEL", previsto no PDTI 2012-2013, não foi atingido integralmente, visto que os "critérios" mencionados no referido objetivo não foram estipulados. Desta forma, com intuito de contribuir para o alcance das metas institucionais, emitimos a seguinte recomendação:

Recomendação nº 10:

Recomendamos que sejam definidos e instituídos os critérios de prioridade e atendimento de demandas para o desenvolvimento de sistemas de informação na UFPEL, conforme objetivo previsto no PDTI 2012-2013.

4. MANIFESTAÇÃO DO GESTOR

As constatações e recomendações deste relatório foram previamente apresentadas ao gestor, que através do Memorando 05/2016 – CTI, manifestou-se da seguinte forma:

"(...) Em que pese a segurança da informação transcender à área de TI, esta Coordenação de Tecnologia da Informação da UFPel, seguindo orientações dos órgãos federais de controle e legislação vigente, tem se empenhado para fomentar e implementar boas práticas de segurança de TI na Universidade, procurando atender dentro de suas competências, as demandas da instituição.

Assim, conforme observado pela auditoria realizada, diversas são as ações que estão sendo incentivadas e promovidas por esta Coordenação de TI para colaborar no cumprimento das exigências dos Órgãos de Controle, em especial neste caso, com a Auditoria Interna da Universidade Federal de Pelotas.

Desta forma, dentro de nossas competências, esta Coordenação continuará perseverando na indução e/ou construção e acompanhamento de Ações e Projetos relacionados à Segurança da Informação na UFPel especialmente as que são relativas às recomendações da AUDIN, bem como, colocamo-nos a disposição desta e de outras unidades da Universidade a fim de realizar intercâmbio com áreas envolvidas como Gestão de Pessoas, Ouvidoria e Gabinete do Magnífico Reitor."

5. CONCLUSÃO

É inquestionável que a área de Tecnologia da Informação desempenha papel fundamental no âmbito desta Universidade. A maioria das atividades realizadas por servidores e alunos depende de ativos de TI. Diante disso, é importante que a gestão concentre esforços em iniciativas que promovam o aperfeiçoamento dos serviços de TI prestados à comunidade acadêmica.

Neste sentido, o tema "Segurança da Informação" merece atenção especial, pois a adulteração, indisponibilidade ou o vazamento de informações podem comprometer significativamente o andamento dos processos institucionais.

Desta forma, apesar de terem sido realizadas diversas ações ligadas ao tema nesta Instituição, tais como a implementação do Comitê de Segurança da Informação, a capacitação de servidores e o oferecimento de palestras e fóruns, entendemos que alguns aprimoramentos precisam

ser realizados como medida de fortalecimento dos controles internos, conforme recomendações emitidas no presente relatório.

Também foi verificado o cumprimento dos objetivos previstos no Plano Diretor de Tecnologia da Informação – PDTI no tocante ao desenvolvimento de sistemas. O resultado foi satisfatório, visto que de forma geral os objetivos foram alcançados.

É importante salientar que a adoção das recomendações emitidas neste relatório fica a critério da gestão, visto que a Auditoria Interna é um órgão de assessoramento técnico e não possui natureza vinculante.

Por fim, destaca-se que este relatório não possui o intuito de esgotar as possibilidades de inconsistências que possam existir, mas sim de subsidiar as decisões administrativas a fim de racionalizar as ações de controle, fortalecer e assessorar a gestão da Universidade.

Pelotas, 05 de fevereiro de 2016.

Letícia dos Passos Pereira Dias
Auditora
Unidade de Auditoria Interna - UFPel

De acordo,

Carlos Arthur Saldanha Dias
Auditor
Chefe da Unidade de Auditoria Interna - UFPel