MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PAMPA
AUDITORIA INTERNA

RELATÓRIO DE AUDITORIA INTERNA N° 04/2015

AUDITORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SUMÁRIO

1. APRESENTAÇÃO

A auditoria de Tecnologia da Informação e Comunicação foi prevista no PAINT 2015, ação 04, Tecnologia da Informação e Comunicação – NTIC, resultante da matriz de análise de processos críticos da AUDIN, realizada em 2013, que definiu os processos/áreas para fins de auditoria em 2014 e 2015.

Ao NTIC compete planejar, organizar, dirigir e controlar as atividades de interesse comum relacionadas à tecnologia da informação e comunicação de acordo com as diretrizes da Universidade. É um órgão estratégico e essencial para eficiência e eficácia da automação dos processos de negócio meio e fim da instituição.

Os gestores - seja em funções de TIC ou não - devem colaborar e trabalhar em conjunto a fim de garantir que a TIC esteja inclusa na abordagem de governança e gestão. Nesse sentido, esta Auditoria tem como objetivo verificar aspectos de Governança e de Gestão de TIC na Instituição, sugerindo possíveis melhorias nos processos.

2. ESCOPO

O escopo desta Auditoria deu-se através da seleção de questões consideradas mais relevantes do questionário do Levantamento de Governança de TI de 2014, realizado pelo Tribunal de Contas da União (iGovTI 2014). Serão examinados os seguintes aspectos:

- ✓ Existência de política de governança em TIC implementada na Instituição.
- ✓ Alcance e alinhamento entre as metas propostas no PDTIC e no PDI.
- ✓ Existência de estrutura de Segurança da Informação e das Comunicações na Instituição.
- ✓ Forma de realização dos processos de aquisição de bens e serviços de TIC, de maneira a agregar valor aos objetivos Institucionais.
- ✓ Execução de gestão de serviços e projetos de TIC, bem como processo de software.

3. INTRODUÇÃO

3.1. Equipe de trabalho

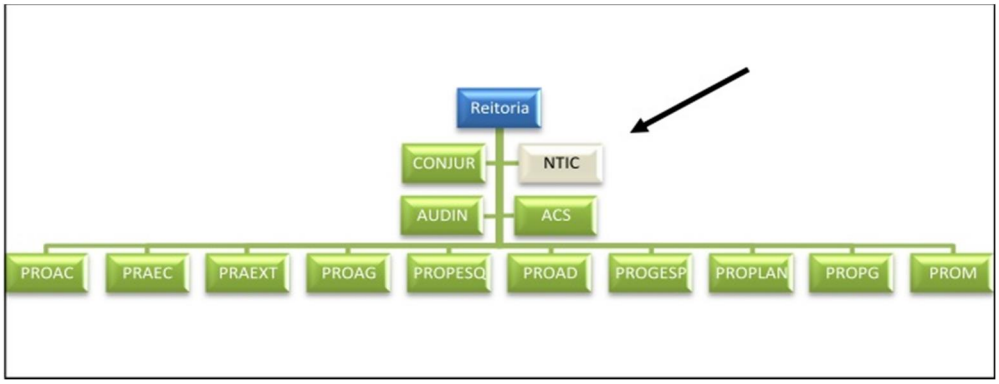
Nome	Cargo	Auditoria
Gabriela Giacomini de Macedo	Auditora	Auditora
Frank Sammer Beulck Pahim	Administrador	Coordenador de auditoria
Ivani Soares	Secretária Executiva	Revisora Textual

3.2. Visão geral do objeto

3.2.1. Estrutura organizacional

O Núcleo de Tecnologia da Informação e Comunicação está previsto no artigo 53 do Regimento Geral da UNIPAMPA e é órgão suplementar da Reitoria, com estrutura prevista na Portaria Institucional nº 745, de 13 de abril.

Figura 1 – Caracterização do NTIC na Instituição



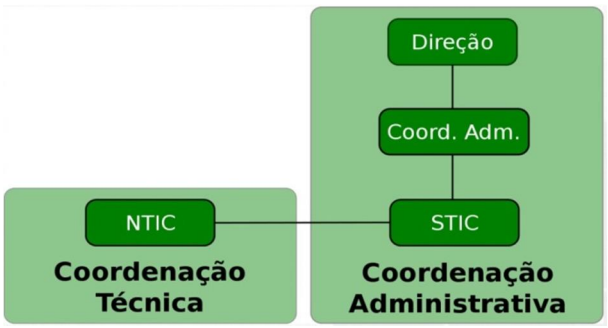
FONTE: PDTIC 2011-2015

3.2.2. Setores de Tecnologia da Informação e Comunicação - STICs

Ficam sob a orientação do NTIC os Setores de Tecnologia da Informação e Comunicação (STICs) das Unidades quanto à aplicação das políticas, normas, padronizações e planejamento referente à área de Tecnologia da Informação e Comunicação da instituição. Porém, hierárquico-administrativamente os STICs respondem às respectivas Direções das Unidades, cabendo respeitar e aplicar as diretrizes do NTIC.

Os STICs têm como principal finalidade planejar, organizar e executar as atividades necessárias ao atendimento das demandas locais de suporte e infraestrutura de tecnologia.

Figura 2 – Localização dos STICs na estrutura



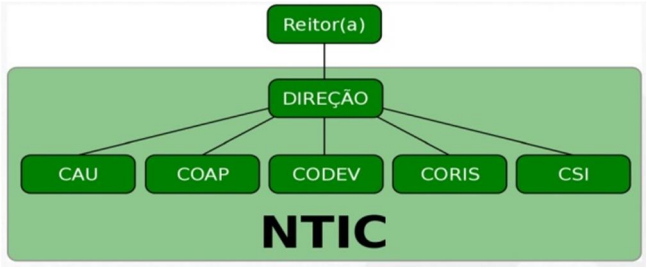
FONTE: Curso Infraestrutura, Conectividade e Gestão de TI na UNIPAMPA

3.2.3. Coordenadorias

O NTIC atualmente está estruturado em cinco Coordenadorias:

- ✓ CAU: Coordenadoria de Apoio ao Usuário
- ✓ COAP: Coordenadoria de Administração e Planejamento
- ✓ CODEV: Coordenadoria de Desenvolvimento
- ✓ CORIS: Coordenadoria de Redes, Infraestrutura e Suporte
- ✓ CSI: Coordenadoria de Segurança da Informação

Figura 3 – Estrutura do NTIC



FONTE: Curso Infraestrutura, Conectividade e Gestão de TI na UNIPAMPA

A Coordenadoria de Apoio ao Usuário e a Direção estão instaladas na Reitoria, em Bagé. As Coordenadorias de Administração e Planejamento, de Desenvolvimento, de Redes, de Infraestrutura e Suporte e de Segurança da Informação estão instaladas em Alegrete.

3.2.4. Estrutura de Governança

A Governança de TIC na Instituição é representada pelo Conselho Gestor de TIC - CGTIC, que é o órgão máximo do Núcleo de Tecnologia da Informação e Comunicação, com competências normativas, deliberativas e consultivas sobre a Política Geral de Tecnologia da Informação e Comunicação na Universidade. Suas competências, de acordo com o Artigo 10 da Resolução nº 019/2010, são:

> I. Estabelecer, em consonância com as normas superiores da Universidade, diretrizes gerais de temas na área de Tecnologia da Informação e Comunicação da Universidade, supervisionando sua execução por meio de regulamentos e instruções;
>
> II. Elaborar, aprovar e, caso necessário, modificar o seu Regimento Interno, em sessão especialmente convocada para este fim, por maioria absoluta dos seus membros para posterior aprovação do CONSUNI;
>
> III. Propor o Plano de Desenvolvimento de Tecnologia da Informação e Comunicação e as suas diretrizes de planejamento e orçamento;
>
> IV. Deliberar sobre as modificações das estruturas internas do NTIC;
>
> V. Acompanhar a implementação e avaliar as políticas de desenvolvimento de pessoal adotadas pela Universidade, no âmbito do NTIC;
>
> VI. Deliberar sobre convênios e contratos de Tecnologia da Informação e Comunicação – TIC;

VII. Decidir sobre matéria omissa neste Regimento; e

VIII. Zelar pelo cumprimento da legislação e das normas institucionais.

O CGTIC deverá ser composto da seguinte maneira, de acordo com o artigo 5º da mesma Resolução:

I. O Diretor do NTIC como seu Presidente, com voto de qualidade além do voto comum;

II. 5 (cinco) servidores docentes da Universidade Federal do Pampa;

III. 5 (cinco) servidores técnico-administrativos em educação da Universidade Federal do Pampa;

IV. 2 (dois) representantes discentes da Universidade Federal do Pampa.

§1º Os membros a que se referem os incisos II e III serão indicados com titulares e respectivos suplentes pelos Conselhos dos Campus, segundo ordem estabelecida pelo NTIC, observando alternância dos Campus na representação dos docentes, técnico-administrativos e discentes.

§2º Os membros titulares e respectivos suplentes, referidos no inciso IV, serão indicados pelo Centro Acadêmico do Campus previsto no sistema de alternância entre Campus.

De acordo com o PDTIC, o Conselho Gestor de TIC é composto pelo grupo do Conselho propriamente dito e apoiado técnica e administrativamente pelos Grupos Assessores (GAs), que são propostos e compostos, sob demanda, a critério do Conselho.

3.3. Definição da Amostra

3.3.1. iGovTI 2014

A amostra definiu, dentre os itens do questionário iGovTI 2014, as questões mais relevantes para análise. Foram selecionadas 43 questões, conforme Anexo I deste Relatório.

3.3.2. Contratação de bens e serviços de TIC

A amostra definiu, dentre o rol de contratos de TIC, aqueles com maior materialidade e relevância.

Quadro 1 – Contratos de TIC selecionados

Nº Contrato	Objeto	Nº Processo
10/2011	Serviços de impressão, digitalização e reprografia.	23100.000004/2011-26
58/2014	Serviços de manutenção de infraestrutura de rede lógica.	23100.001308/2014-53

O processo Nº 23100.001308/2014-53 (Contrato 58/2014) foi analisado na Auditoria de Licitações – PROAD.

3.4. Critérios de análise

- ✓ Legalidade: observância a leis e regulamentos aplicáveis.
- ✓ Eficiência: relação entre bens e serviços gerados por uma atividade e os custos empregados para produzi-los, em um determinado período de tempo, mantidos os padrões de qualidade.
- ✓ Eficácia: alcance das metas propostas no PDTIC e no PDI.
- ✓ Economicidade: capacidade da Instituição em gerir adequadamente os recursos financeiros colocados à disposição da área de TIC.
- ✓ Levantamento de Governança de TI 2014 TCU – iGovTI 2014.

3.5. Metodologia

A principal metodologia de trabalho utilizada nesta Auditoria foi a de análise documental. Através da aplicação de testes substantivos, buscou-se validar as respostas fornecidas pela Instituição às questões consideradas mais relevantes do questionário do iGovTI 2014. Para tanto, foram emitidas as seguintes Solicitações de Auditoria:

Quadro 2 – SAs emitidas

Nº SA	Destinatário	Solicitação	Data resposta
022/2015	Diretor NTIC	Comprovação itens 1.2.c, 1.2.d, 1.3.b, 1.3.c, 1.3.d, 1.7.c, 3.1.b.	07/04 e 13/04
031/2015	Diretor NTIC	Comprovação itens 2.2.a, 2.2.b, 2.2.c, 2.2.f, 2.2.h, 2.2.i.	04/05
044/2015	Diretor NTIC	Comprovação itens 1.7.d, 5.4.a, 5.4.b, 5.4.e, 5.4.i, 5.4.j, 5.4.k, 5.4.o, 5.4.s, 5.4.t, 5.1.c, 5.2.4, 5.5.a, 5.6.b, 5.6.f.	21/05
049/2015	Diretor NTIC	Esclarecimentos adicionais itens 1.2.b e 1.3.b.	28/05
053/2015	Coordenador COAP	Esclarecimentos adicionais item 2.2.h.	29/05
055/2015	Pró-Reitor	Pregão 01/2011 – Processo nº 23100.000004/2011-26	01/06
060/2015	Diretor NTIC	Causas e medidas de prevenção tomadas, com relação ao incidente de Segurança da Informação ocorrido em 2013.	06/07
061/2015	Coordenador COAP	Comprovação dos itens 5.8.b, 5.8.c e 5.9.c, com relação aos Pregões 01/2011, 31/2014 e 35/2014.	01/07

Com o recebimento dos documentos, a Auditoria validou ou não as respostas da Instituição aos itens selecionados do iGovTI 2014.

3.6. Volume de recursos auditados

Com relação aos quesitos de Governança, considerou-se como volume de recursos auditados o valor de R$ 4.944.320,71, montante empenhado pela Instituição em 2014 em itens demonstrados abaixo:

GND (Cod/Abrev)	Elemento Despesa (Cod/Desc)	Sub-elemento Despesa (Cod/Desc)	Empenhado (R$)
3-ODC	30 - MATERIAL DE CONSUMO	33903017 - MATERIAL DE PROCESSAMENTO DE DADOS	227.247,17
3-ODC	30 - MATERIAL DE CONSUMO	33903030 - MATERIAL PARA COMUNICACOES	32.103,94
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903994 - * AQUISICAO DE SOFTWARES	0,00
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903908 - MANUTENCAO DE SOFTWARE	97.500,00
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903995 - MANUT.CONS.EQUIP. DE PROCESSAMENTO DE DADOS	32.533,16
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903911 - LOCACAO DE SOFTWARES	7.650,00
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903957 - SERVICOS TECNICOS PROFISSIONAIS DE T.I.	2.450,00
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903997 - COMUNICACAO DE DADOS.	424.789,59
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903958 - SERVICOS DE TELECOMUNICACOES	224.329,80
3-ODC	39 - OUTROS SERVICOS DE TERCEIROS - PJ	33903983 - SERVICOS DE COPIAS E REPRODUCAO DE DOCUMENTOS	392.189,26
4-INV	52 - EQUIPAMENTOS E MATERIAL PERMANENTE	44905235 - EQUIPAMENTOS DE PROCESSAMENTO DE DADOS	3.396.511,94
4-INV	39 - OUTROS SERVICOS DE TERCEIROS - PJ	44903993 - AQUISICAO DE SOFTWARE	6.327,00
4-INV	52 - EQUIPAMENTOS E MATERIAL PERMANENTE	44905206 - APARELHOS E EQUIPAMENTOS DE COMUNICACAO	100.688,85

Fonte: Portal SIGA Brasil

Com relação aos processos utilizados para responder às questões 5.7.a, 5.7.b, 5.7.c, 5.7.f, 5.7.i, 5.8.b, 5.8.c, 5.9.b e 5.9.c:

Quadro 3 – Volume de recursos auditados

N° PROCESSO	VALOR
23100.001308/2014-53	R$ 481.070,72
23100.000004/2011-26	R$ 1.129.262,35
TOTAL	**R$ 1.610.333,07**

3.7. Resultados Esperados com a Auditoria

Validar o atual patamar de Governança e de Gestão de TIC em que se encontra a Instituição, sugerindo possíveis melhorias nos processos.

4. CONSIDERAÇÕES: VALIDAÇÃO DAS RESPOSTAS DO IGOVTI 2014

Abaixo consta o quadro demonstrativo de validação das respostas do questionário do iGovTI2014 e logo após o detalhamento e considerações da Auditoria para cada item.

Quadro 4 – Demonstrativo de validação das respostas

Item iGovTI2014	Situação verificada na Auditoria
1.2.b.	Resposta validada
1.2.c.	Resposta validada
1.2.d.	Resposta não validada
1.3.b.	Resposta não validada
1.3.c.	Resposta validada
1.3.d	Resposta validada*
1.7.c.	Item melhorado
3.1.b.	Resposta validada
2.2.a.	Resposta validada
2.2.b.	Resposta validada
2.2.c.	Resposta validada
2.2.e.	Resposta validada
2.2.f.	Resposta não validada
2.2.h.	Resposta validada
2.2.i.	Resposta validada
1.7.d.	Item melhorado
5.4.a.	Resposta validada*
5.4.b.	Resposta validada*
5.4.d.	Item melhorado
5.4.e.	Resposta validada*
5.4.i.	Item melhorado
5.4.j.	Resposta validada
5.4.k.	Resposta validada
5.4.o.	Resposta validada
5.4.s.	Resposta validada
5.4.t.	Resposta validada
5.7.a.	Resposta validada
5.7.b.	Resposta validada
5.7.c.	Resposta não validada
5.7.f.	Resposta não validada
5.7.i.	Resposta validada
5.8.b.	Resposta validada
5.8.c.	Resposta não validada
5.9.b.	Resposta validada
5.9.c.	Resposta validada*
5.1.a.	Resposta validada*
5.1.c.	Resposta validada
5.2.a.	Resposta validada*
5.3.a.	Resposta validada

Item iGovTI2014	Situação verificada na Auditoria
1.2.b.	Resposta validada
1.2.c.	Resposta validada
1.2.d.	Resposta não validada
1.3.b.	Resposta não validada
1.3.c.	Resposta validada
1.3.d	Resposta validada*
1.7.c.	Item melhorado
3.1.b.	Resposta validada
2.2.a.	Resposta validada
2.2.b.	Resposta validada
2.2.c.	Resposta validada
2.2.e.	Resposta validada
2.2.f.	Resposta não validada
2.2.h.	Resposta validada
2.2.i.	Resposta validada
1.7.d.	Item melhorado
5.4.a.	Resposta validada*
5.4.b.	Resposta validada*
5.4.d.	Item melhorado
5.4.e.	Resposta validada*
5.4.i.	Item melhorado
5.5.a.	Resposta validada
5.6.a.	Item melhorado
5.6.b.	Item melhorado
5.6.f.	Resposta validada

Resposta validada: a Auditoria, após verificação, concluiu que a resposta da Instituição estava adequada à realidade dos fatos.

Resposta validada*: Respostas que, apesar de validadas, não sofreram evolução (prática adotada parcialmente/prática não adotada).

Resposta não validada: a Auditoria, após verificação, concluiu que a resposta da Instituição não estava adequada à realidade dos fatos, dando origem a constatações neste Relatório.

Item melhorado: a Auditoria, após verificação, concluiu que a situação da Instituição melhorou, saindo de uma prática não adotada/adotada parcialmente para prática adotada integralmente.

4.1. Questão: **A organização dispõe de um comitê de TI formalmente instituído, composto por representantes de áreas relevantes da organização.** (Item: **1.2.b.**)

4.1.1. Resposta da Instituição: **Prática adotada: integral**

4.1.2. Solicitação de comprovação: Documento que formalizou o atual Comitê de TI e informações sobre os participantes do Comitê de TI e das áreas das quais eles fazem parte, inclusive áreas de negócio. (SA 049/2015)

4.1.3. **Resposta NTIC** (Memorando 061/2015):

Em conformidade com os parágrafos 1º e 2º do Art. 5º do Regimento do Núcleo de Tecnologia da Informação e Comunicação da UNIPAMPA (1), que dispõe sobre a estrutura geral do Comitê de TI, iniciou-se em 2013 a recomposição do CGTIC (após a desmobilização causada pela greve de servidores técnico-administrativos e docentes de 2012) com o envio de solicitações formais às direções dos campi para indicação dos membros titulares e suplementes que posteriormente formariam a atual composição do Conselho. Em anexo (**Anexo 1**) estão os memorandos recebidos pelas direções com as respectivas indicações.

Apresentamos no **Anexo 2** o quadro com a atual composição do Conselho e detalhamento dos cargos e áreas de atuação de cada membro titular e suplente. Adiantamos que atualmente o NTIC está em contato com as direções dos campi Jaguarão e Alegrete solicitando nova indicação para os respectivos membros que não possuem representação, assim como para novas indicações para membros no qual estejam no final de seu mandato.

(1) http://porteiras.r.unipampa.edu.br/portais/consuni/files/2010/06/Res.-19_2010-Regimento-NTIC.pdf

4.1.4. **Análise da Auditoria:**

Na UNIPAMPA, o Comitê de TI é intitulado de Conselho Gestor de Tecnologia da Informação e Comunicação – CGTIC, e é composto por: Diretor do NTIC; cinco servidores docentes da UNIPAMPA e suplentes; cinco servidores técnico-administrativos em educação da UNIPAMPA e suplentes; dois representantes discentes da UNIPAMPA[1].

O Guia de Comitê de TI do SISP - Sistema de Administração dos Recursos de Tecnologia da Informação [2] informa que o Comitê de TI (CTI) é um órgão colegiado, formado por membros das áreas finalísticas e da área de TI, que tem o objetivo de promover a entrega de valor por meio da TI e do uso estratégico da informação na organização, além de esclarecer que os papéis desempenhados no Comitê de TI não devem ser desempenhados exclusivamente por profissionais da área de TI.

De acordo com o Anexo 2, apresentado pelo NTIC, os cinco membros titulares servidores técnico-administrativos em educação são da área de TI (Técnicos ou Analistas em TI). Os cinco membros titulares servidores docentes são de áreas diversas: Ciência da Computação, Química, Administração, Genética e Biologia Molecular e Desenvolvimento de Sistemas de Informação. Os dois representantes discentes, titular e suplente, respectivamente, são dos cursos de Fisioterapia e Ciências da Natureza. Sendo assim, a resposta ao item 1.2.b foi validada pela Auditoria, pois o CGTIC da UNIPAMPA é composto por membros das áreas finalísticas e da área de TIC.

[1] Artigo 5º da Resolução nº 019/2010.
[2] Guia de Comitê de TI do SISP: versão 2.0/Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação - Brasília: MP, 2013.

4.2. Questão: **O comitê de TI realiza as atividades previstas em seu ato constitutivo.** (Item: **1.2.c.**)

4.2.1. Resposta da Instituição: **Prática adotada: integral**

4.2.2. Análise da Auditoria:

As atividades que competem ao CGTIC estão no artigo 10 da Resolução nº 019/2010. Para validar a resposta a este item, a Auditoria Interna fez a leitura das atas das reuniões do Conselho e analisou os assuntos que vêm sendo tratados.

O CGTIC da UNIPAMPA tem atuado principalmente no estabelecimento de diretrizes gerais de temas na área de TIC e na manutenção e criação de Grupos Assessores em áreas estratégicas. Como exemplo, citamos as deliberações que geraram os documentos Norma de uso de credenciais de acesso[3] e Normas de utilização de e-mail[4].

Observou-se um longo período sem registro de reuniões do Conselho, de 04/11/11 a 16/10/13. De acordo com o parágrafo 1º do art. 8º do Regimento, a periodicidade das reuniões é semestral, e ainda de acordo com registro na Ata nº 9, a periodicidade aprovada pelos membros era quinzenal. Também se constatou que a aprovação do PDTIC, para posterior proposição ao CONSUNI, competência também do CGTIC[5], ocorreu em 2011, com a previsão de ser revisado anualmente[6], porém não há mais registro dessa atividade em atas posteriores.

Apesar do descrito acima, o Conselho Gestor de TIC estava atuando de acordo com suas competências na época de realização do questionário, fazendo com que a Auditoria validasse a resposta ao item 1.2.c.

4.3. Questão: **A organização prioriza as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.** (Item: **1.2.d.)**

4.3.1. Resposta da Instituição: **Prática adotada: integral**

4.3.2. Solicitação de comprovação: Informações sobre a forma de priorização das ações de TI (SA 022/2015).

4.3.3. Resposta NTIC (Memorando 035/2015):

[3] Ata nº 15.
[4] Ata nº 15.
[5] Inciso III, artigo 10, Resolução nº 019/2010.
[6] Ata nº 8.

As ações de TI de ampla abrangência e com propensão a serem transformadas em normas, são encaminhadas para discussão no CGTIC da UNIPAMPA, instituído pela Resolução nº19, de 25 de novembro de 2010(2). Entre suas principais competências está a concepção do PDTIC do quinquênio, em consonância com o PDI da Instituição. Além desta tarefa fundamental, compete ao CGTIC debater e deliberar sobre assunto inseridos na pauta por seus conselheiros, o que eleva a importância dos temas, priorizando-os frente as demais ações não acolhidas no Conselho, para posterior implementação na universidade. No ponto de vista normativo de serviços de TIC institucionais, somente as normas que seguem este fluxo, consolidadas com amparo do CGTIC, são formalmente instituídas e amplamente divulgadas. As publicações são centralizadas no site do NTIC(3).

Complementarmente, há necessidade de ressaltar que as atividades de planejamento estratégicas e táticas do órgão são sempre debatidas em reuniões periódicas semanais dos gestores do NTIC, incluindo diretor, coordenadores e suplentes. As reuniões ocorrem por meio de webconferência, gravadas e com encaminhamentos registrados em documento simplificado de memória das reuniões. Documento este que é usado como referencial para acompanhamento das atividades prioritárias e seus responsáveis. Além disso, cabe destacar o fórum permanente de discussão assíncrona com as equipes dos STICs, denominado NTIC-Unidades. Trata-se de uma lista de discussão na qual são repassadas informações sobre atividades técnico-administrativas que deverão ser seguidas nas unidades, bem como serve de retroalimentação para ações que precisam ser discutidas com os olhares diferenciados daqueles que atuam diariamente com os usuários finais dos serviços de TIC.

(2) http://porteiras.r.unipampa.edu.br/portais/consuni/files/2010/06/Res.-19_2010-Regimento-NTIC.pdf

(3) http://ntic.unipampa.edu.br/conselho-gestor-de-tic/normas/

4.3.4. Análise da Auditoria:

De acordo com o Guia de Comitê de TI do SISP, em relação aos direcionamentos dados pelo Comitê (de TI), temos como exemplos: a definição de prioridades para os projetos e ações de TI, a tomada de decisão em relação aos recursos orçamentários para a viabilização da implementação dos planos e a deliberação sobre as estratégias, planos e políticas de TI para toda a organização.

Ainda na Nota Técnica nº 7, do TCU[7], espera-se que o comitê de TI tenha, entre suas responsabilidades, atuar na aprovação e na alocação de recursos destinados à TI; na priorização de ações e projetos de TI; no acompanhamento da execução das estratégias e planos de TI; na comunicação à alta administração de informações gerenciais de TI.

Através da resposta exposta no Memorando 035/2015 e da leitura das Atas das Reuniões do CGTIC, não foi possível evidenciar que o Conselho Gestor esteja atuando como instância consultiva com relação à priorização das ações de TI na Instituição. Salienta-se que a questão 1.2.d leva em consideração o Comitê como órgão consultivo, não apenas normativo. Por esses motivos, a resposta ao item 1.2.d não foi validada pela Auditoria.

[7] Nota Técnica 7/2014 - Sefti/TCU – versão 2.8.

4.4. Questão: **A organização define formalmente diretrizes para gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária.** (Item: **1.3.b.**)

4.4.1. Resposta da Instituição: **Prática adotada: integral**

4.4.2. Solicitação de comprovação: Informações sobre as diretrizes para gestão do portfólio de projetos e serviços de TI definidas pela Instituição e como foram formalizadas (SA 022/2015) e informação sobre como são formalizadas as decisões tomadas nas referidas reuniões com a alta gestão (SA 049/2015).

4.4.3. **Resposta NTIC**:

Memorando 035/2015 – Resposta à SA 022/2015:

O NTIC adota como referência estratégica, de forma contínua e permanente, o Plano Diretor de Tecnologia da Informação e Comunicação da UNIPAMPA(4) para gestão do portfólio de projetos e serviços de TI. Todavia, a priorização das ações de TI é continuamente replanejada e reavaliada junto com a alta gestão da Universidade, a partir de reuniões periódicas semanais com reitora, vice-reitor e pró-reitores, com o intuito de mantê-las alinhadas com as atuais demandas e anseios da comunidade acadêmica.

Por meio da previsão orçamentaria do setor, incluído no orçamento da universidade para elaboração do Projeto de Lei Orçamentaria Anual da União, são consolidadas as despesas para execução do planejamento realizado, juntamente com a Pró-Reitoria de Administração e Pró-Reitoria de Planejamento, Desenvolvimento e Avaliação.

(4) http://ntic.unipampa.edu.br/quem-somos-2/pdtic/

Memorando 061/2015 – Resposta à SA 049/2015:

As deliberações, envolvendo aspectos de TIC, realizadas juntamente com a alta gestão, principalmente nas reuniões semanais das quais participam reitora, vice-reitor, pró-reitores, chefe de gabinete e direção do NTIC, são repassadas imediatamente aos coordenadores das equipes do núcleo por meio de ferramentas de comunicação síncronas (normalmente chat) ou e-mail. Em casos especiais, reuniões virtuais, por meio de ferramenta de web ou videoconferência, são especificamente agendadas para esclarecimentos de detalhes que envolvem os projetos. Desta forma, a ordem com que os projetos são executados pelo NTIC fica flexibilizada, atendendo as necessidades da instituição. A dinâmica resultante deste processo permite que o andamento da execução dos projetos prioritários seja acompanhado pela direção por meio das reuniões semanais com os coordenadores do núcleo, os quais coletivamente deliberam sobre alternativas capazes tornar mais eficiente a execução destes projetos. As memórias das reuniões de 2015 estão disponibilizadas no **Anexo 3**.

A título de exemplo encaminhamos no **Anexo 4** alguns encaminhamentos com origem de reuniões com a alta gestão, repassados às equipes do núcleo utilizando a comunicação digital, considerada como oficial no setor.

4.4.4. **Análise da Auditoria:**

De acordo com a Nota Técnica nº 7 do TCU, questões importantes relacionadas à alocação de recursos, à realização de investimentos e à priorização de projetos de TI são tipicamente decididas por estruturas organizacionais, a exemplo da alta administração e do comitê de TI.

Sobre a priorização de projetos e demandas, o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC apresenta em que foi baseada:

- Reuniões da alta Gestão da Instituição;
- Discussões técnicas e administrativas;
- Levantamento e análise de demanda das diferentes áreas e setores da Instituição;
- Identificação e tratamento de questões críticas de implantação da Instituição;
- Disponibilidade de recursos orçamentários;
- Disponibilidade de recursos humanos;
- Qualificação, capacitação e domínio técnico das tecnologias envolvidas no projeto/demanda por parte da equipe envolvida;
- Avaliação macro dos riscos de sucesso do projeto/demanda;
- Estruturação do atendimento dos projetos e demandas em diferentes fases, sendo normalmente duas (fase I: pesquisa, formação e experimentação; e fase II: planejamento e implantação definitiva da solução e/ou serviço);
- Avaliação de tecnologias e recursos tecnológicos maturados e amplamente utilizados no mercado, evitando riscos de fracasso dos projetos e demandas;
- Pesquisas e avaliações de soluções e alternativas tecnológicas junto a outras Instituições, fornecedores e fabricantes.

O PDTIC, nas páginas 61 a 110, traz o Portfólio de Projetos da área de TIC e esclarece que, em uma nova fase pós-concepção, a definição das prioridades será realizada em conjunto com a Gestão da Instituição, gerando um mapa de priorização de projetos de acordo com o Mapa de Riscos, apresentado também no PDTIC. Porém, diferentemente do que foi previsto no documento, nenhuma revisão anual foi divulgada, nem o mapa de priorização de projetos baseado nas novas definições.

Através das memórias de reuniões, apresentadas nos anexos do Memorando 061/2015, foi possível verificar que foram decididos os projetos a serem priorizados, mas não constam os critérios utilizados para a priorização. As reuniões semanais com a Reitora, Vice-Reitor e Pró-Reitores são as formas utilizadas pelo NTIC para realinhar o PDTIC às prioridades atuais da Instituição. Ainda assim, persiste o fato de que não há uma formalização de diretrizes para gestão do portfólio.

Sendo assim, a resposta ao item 1.3.b não foi validada pela Auditoria, sendo considerada como adotada parcialmente. Como boa prática, demonstra-se o que é adotado na Metodologia de Gerenciamento de Portfólio de Projetos do SISP[8]. Uma das fases apresentadas na construção do portfólio é a fase chamada de “Priorizar projetos”, que tem como saída a Planilha de Portfólio de Projetos com os projetos priorizados, e também os critérios de Priorização.

[8] Metodologia de Gerenciamento de Portfólio de Projetos do SISP/Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação – Brasília: MP, 2013.

4.5. Questão: **A organização define formalmente diretrizes para contratação de bens e serviços de TI.** (Item: **1.3.c.**)

4.5.1. Resposta da Instituição: **Prática adotada: integral**

4.5.2. Solicitação de comprovação: Informações sobre as diretrizes para contratação de bens e serviços de TI e como foram formalizadas (SA 022/2015).

4.5.3. **Resposta NTIC** (Memorando 035/2015):

O processo de contratação de bens e serviços de TI segue a Instrução Normativa Nº 04/2010[5], revisada em 2014 e publicada pela Secretaria de Logística e Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão, e dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática - SISP do Poder Executivo Federal. O Tribunal de Contas da União avaliza esta normativa no Guia de Boas Práticas em Contratação de Soluções de TI, publicado em 2012[6].

O NTIC mantém uma página na Internet com orientações, atualizadas anualmente, acerca de contratações de TI no âmbito da universidade, elaborado com base nas publicações supracitadas e esclarecendo todas as etapas do processo[7].

Seguindo a IN 04/2014, todas as demandas de TI registradas formalmente são analisadas pelo NTIC, para revisão técnicas das especificações e decisão sobre a inclusão do bem no rol de licitações. Para tanto, um dos requisitos é o alinhamento do bem ou serviço com os objetivos institucionais demonstrados no PDI da universidade, assim como estar contemplado na previsão orçamentaria da unidade demandante.

(5) http://www.governoeletronico.gov.br/sisp-conteudo/nucleo-de-contratacoes-de-ti/modelo-de-contratacoes-normativos-e-documentos-de-referencia/instrucao-normativa-mp-slti-no04
(6) http://portal2.tcu.gov.br/portal/pls/portal/docs/2511467.PDF
(7) http://ntic.unipampa.edu.br/compras/

4.5.4. **Análise da Auditoria:**

No PDTIC está definida como principal diretriz para contratação de bens e serviços de TIC a Instrução Normativa nº 04. Além disso, a Coordenadoria de Administração e Planejamento – COAP elaborou e publicou o Guia de Compras de Itens de Tecnologia da Informação e Comunicação, que consolida as normativas expedidas pela SLTI/MPOG quanto ao devido processo de compras de itens de TIC. Sendo assim, a resposta ao item 1.3.c. foi validada pela Auditoria.

4.6. Questão: **A organização define formalmente diretrizes para avaliação do desempenho dos serviços de TI.** (Item: **1.3.d.**)

4.6.1. Resposta da Instituição: **Prática adotada: parcial**

4.6.2. Solicitação de comprovação: Informações sobre as diretrizes para avaliação do desempenho dos serviços de TI e como foram formalizadas (SA 022/2015).

4.6.3. **Resposta NTIC** (Memorando 035/2015):

O NTIC, em alinhamento com os demais setores da instituição, busca o aprimoramento do acompanhamento dos serviços de TIC por meio de diferentes instrumentos, tais como: (i) formalização e divulgação, para a comunidade interna e externa, de suas principais metas por meio da inclusão de metas específicas de TIC no PDI[8]; (ii) divulgação de relatórios com níveis de disponibilidade de sistemas, estatísticas de atendimentos de chamados, indicadores de atendimento de requisitos de sistemas, entre outros[9]; e (iii) questionários eletrônicos enviados a comunidade para avaliação periódica dos serviços continuados - contratos de telefonia, impressão, etc.

(8) http://porteiras.r.unipampa.edu.br/portais/consuni/files/2010/06/Res.-71_2014-PDI.pdf

(9) http://ntic.unipampa.edu.br/relatorios/

4.6.4. Análise da Auditoria:

O PDTIC em validade atualmente na Instituição foi elaborado baseado no Plano de Desenvolvimento Institucional – PDI 2009 a 2013 da UNIPAMPA. Nesse PDI, havia a definição de objetivos, com as respectivas estratégias e metas. A área de TIC estava envolvida tanto em estratégias quanto em metas de vários objetivos.

Porém, no atual PDI da Instituição, para o período de 2014 a 2018, constam iniciativas e indicadores para a área de TIC sem formalização de metas a serem atingidas. Logo, não há parâmetros para comparar os resultados alcançados dos serviços de TIC, não sendo possível avaliar o desempenho.

Já no PDTIC, as iniciativas estão especificadas em metas macro, indicadores e metas anuais, através do Balanced Scorecard. Nas Tabelas 3, 11 e 16[9] são definidas as principais metas com relação à qualidade dos serviços de TIC. Porém, ressalta-se que os valores dos indicadores deveriam sofrer revisão detalhada em meados de 2012, o que não ocorreu.

Sendo assim, considera-se que a prática do item 1.1.d continua sendo adotada parcialmente.

4.7. Questão: **A organização realiza avaliação periódica de sistemas de informação.** (Item: **1.7.c.**)

4.7.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.7.2. Solicitação de comprovação: Informações sobre a existência de avaliações, incluídas na planilha sobre os sistemas de informação (SA 022/2015).

4.7.3. Resposta NTIC (Memorando 039/2015):

O NTIC adota como sistemática a revisão dos sistemas de informação a partir de dados gerados por ferramentas de monitoramento e registro de ocorrências relacionadas aos sistemas em uso na universidade. [...]

A Coordenadoria de Segurança da Informação (CSI) mantém o serviço de monitoramento dos sistemas de informação. A partir dos relatórios gerados pelo software livre Zabbix os dados são utilizados pela CAU e CODEV para acompanhar a disponibilidade e performance dos sistemas.

[9] Páginas 34, 43 e 48, respectivamente (PDTIC UNIPAMPA – fevereiro 2011).

É com base nas informações geradas por estas ferramentas que o NTIC mantém avaliações constantes nos sistemas de informação da UNIPAMPA, aplicando atualizações com o objetivo de proporcionar maior eficiência aos processos informatizados, com foco no atendimento às expectativas dos usuários.

4.7.4. Análise da Auditoria:

Através do curso "Infraestrutura, Conectividade e Gestão de TI na UNIPAMPA", no qual parte da equipe de Auditoria se fez presente, foi apresentado o funcionamento do software Zabbix. Essa ferramenta faz o monitoramento de desempenho (ativos de rede) e de disponibilidade (serviços), coletando dados, analisando-os e tomando ações com base nos eventos encontrados.

Através do link http://ntic.unipampa.edu.br/relatorios/disponibilidade-2/, é possível acessar alguns Relatórios de Disponibilidade, os quais confrontam ocorrências de problemas com disponibilidades dos Sistemas (%). Sendo assim, a Auditoria considera que a Instituição saiu da situação de prática não adotada para prática adotada integralmente no item 1.7.c.

4.8. Questão: **Os principais processos de negócio da organização são suportados por sistemas informatizados.** (Item: **3.1.b.**)

4.8.1. Resposta da Instituição: **Prática adotada: integral**

4.8.2. Solicitação de comprovação: Relação dos principais sistemas e sua relação com a área de negócio da Universidade, em uma planilha de informação com, no mínimo, as seguintes informações: área atendida/sistema/situação atual (atualização do sistema) /previsão para atualização/número de usuários (SA 022/2015).

4.8.3. Resposta NTIC (Memorando 039/2015):

O principal processo da organização, referente ao controle acadêmico, utiliza como sistema informatizado a plataforma SIE, desde 2008 sob manutenção deste núcleo. Entretanto, as funções deste sistema estão sendo gradativamente migradas para o novo ERP[1] da universidade, desenvolvido no NTIC e já em ampla utilização. Este novo sistema, denominado Sistema GURI - Sistema de Gestão Unificada de Recursos Institucionais, deverá abranger e informatizar todos os processos acadêmicos e administrativos da universidade. Atualmente possui 24 módulos em uso por diversos setores da instituição, cada qual com sua função específica.

Enviamos em anexo a relação dos sistemas de informação em uso na UNIPAMPA, com detalhamento complementar.

(1) Sigla derivada do nome Enterprise Resource Planning, que define softwares que integram todos os dados e processos de uma organização em um único sistema.

4.8.4. Análise da Auditoria:

A existência de interação entre os processos de negócio da organização e uma rede de sistemas de informação é um fator determinante para a produção de indicadores e instrumentos de controle efetivo para um constante monitoramento das atividades da Instituição.

Na tabela enviada em anexo, com informações sobre os sistemas de informação em uso da UNIPAMPA, de 2008 a 2015, verificou-se que os sistemas abrangem vários setores da Instituição. Foram apresentados 41 sistemas de informação em uso. Cerca de 40% deles atende

áreas diretamente ligadas a ensino, pesquisa e extensão, enquanto os demais atendem áreas administrativas. Por esse motivo, a Auditoria validou a resposta da UNIPAMPA ao item 3.1.b.

4.9. Questão: **A organização executa periodicamente processo de planejamento de TI.** (Item: **2.2.a.**)

4.9.1. Resposta da Instituição: **Prática adotada: integral**

4.9.2. Solicitação de comprovação: Última versão revisada do PDTIC (SA 031/2015).

4.9.3. **Resposta NTIC** (Memorando 043/2015):

A versão mais recente do PDTI da universidade [...] foi publicado em fevereiro de 2011 com base nos macro projetos institucionais apresentados no PPI e PDI vigentes à época, estipulando metas até 2015.

Entretanto, considerando a dinamicidade de instituições federais de ensino superior, principalmente quando se encontram em processo de implantação, aliado às evoluções tecnológicas e a interferência de fatores externos, especialmente de disponibilidade orçamentária, o planejamento de TI exige revisões com menores intervalos de tempo. O que vem ocorrendo na gestão atual do núcleo, através de planejamentos trimestrais consolidados entre as coordenadorias e a direção, além das reuniões periódicas semanais com o Gabinete da Reitora, Vice-Reitor e Pró-Reitores, bem como nas reuniões mensais com as direções de unidades, onde oportunamente foram tratadas a priorização de demandas específicas ou comuns de forma a moldar o planejamento do núcleo ao atendimento destas necessidades.

Embora não tenha se traduzido em alterações formais do PDTI, todas as alterações de rumo que foram feitas ao longo destes anos foram feitas com base em decisões colegiadas e amparadas pelas raízes do PDTI.

No entanto, o planejamento trimestral ocorrido desde 2014, já aponta para o início da revisão do conteúdo do PDTI em 2015, com base em orientações atualizadas, como o Guia de Elaboração de PDTI do SISP (2). Além da proximidade do término de vigência, a revisão está sendo realizada este ano, sobretudo, pela publicação do PDI atualizado da Universidade e da recomposição do Conselho Gestor de TIC, órgão que deve estar envolvido no processo, conforme orientações preconizadas pelo SISP (3) e TCU (4). [...]

(2)http://sisp.gov.br/guiapdti/wiki/download/file/Guia_de_Elabora%C3%A7%C3%A3o_de_PDTI_v1.0_-_versao_digital_com_capa.pdf

(3) Guia de Elaboração de PDTI, SISP, 2012, pág. 22.

(4) Acórdãos 2023/2005-P, 1603/2008-P e 2308/2010-P, do TCU.

4.9.4. **Análise da Auditoria:**

O PDTIC atual corresponde à primeira versão, elaborada em 2011. De acordo com o documento[10], "por ter um horizonte de 5 anos, torna-se necessária a revisão periódica para os refinamentos. Portanto, a revisão será anual [...]". Sendo assim, o planejamento ainda está em validade até o final de 2015, porém não foram publicadas as revisões anuais.

Considerando a época do questionário (2014), a resposta ao item está apropriada e foi validada pela Auditoria, pois o processo de planejamento – PDTIC - é executado periodicamente (foi realizado em 2011 e o próximo deverá entrar em vigor em 2016). Além disso, de acordo com o

[10] PDTIC UNIPAMPA – fevereiro 2011 – Página 157.

Memorando 043/2015, com o intuito de revisar o planejamento de TIC, são realizadas reuniões semanais com a Alta Gestão, reuniões mensais com as Direções das Unidades e planejamentos trimestrais entre as Coordenadorias e a Direção do NTIC.

4.10. Questão: **O processo de planejamento de TI prevê a participação das áreas mais relevantes da organização.** (Item: **2.2.b.**)

4.10.1. Resposta da Instituição: **Prática adotada: integral**

4.10.2. Solicitação de comprovação**:** Metodologia adotada para obter a participação das áreas estratégicas (SA 031/2015).

4.10.3. **Resposta NTIC** (Memorando 043/2015):

[...] a direção do núcleo se reúne periodicamente com a alta gestão da instituição como também com as direções dos campi, apresentando projetos institucionais de ampla abrangência para discussões ou acolhendo demandas específicas por meio das manifestações dos dirigentes. Tais tratativas posteriormente se transformam em pauta das reuniões periódicas síncronas, semanais, realizadas com as coordenações do NTIC, visando planejar e sincronizar ações em nível tático, de acordo com as competências e atribuições complementares das coordenadorias.

O CGTIC possui papel importante no planejamento, sua formação possui representantes das áreas finalísticas e da área de TI e sua principal tarefa é zelar para que a formulação e a implementação das estratégias e planos de TI estejam harmonizadas com os objetivos organizacionais de alto nível (6).

(6) Guia para criação e funcionamento do Comitê de TI, SISP, 2013, pág. 12.

4.10.4. **Análise da Auditoria:**

De acordo com o Guia de PDTI do SISP[11], o Planejamento de TI deve ser elaborado com a participação das diversas unidades da área de TI e das áreas finalísticas, e os papéis envolvidos no ciclo de vida do PDTI não devem ser desempenhados exclusivamente por profissionais da área de TI. Pelo contrário, é essencial que a elaboração e o acompanhamento do PDTI ocorram com a participação das diversas áreas do órgão – finalísticas e meio.

O Guia também apresenta a figura da Equipe de Elaboração do PDTI: "é quem operacionaliza o projeto de elaboração do PDTI. Os membros da equipe são designados pelo Comitê de TI, que deve indicar servidores tanto das áreas finalísticas quanto da área de TI. Ou seja, reforça-se a orientação de que os profissionais que vão participar da elaboração do PDTI não sejam exclusivamente servidores da área de TI. Outra recomendação é que a equipe não seja técnica, mas primordialmente negocial, com conhecimento multidisciplinar, perfil colaborativo e integrador, domínio da cultura organizacional e do negócio da sua área". Essa equipe de elaboração, apresentada na página 03 do PDTIC da UNIPAMPA, conta com membros da área de TIC e de negócio da Instituição.

Também de acordo com o exposto no Memorando 043/2015, são realizadas reuniões periódicas com áreas estratégicas da Instituição, no intuito de planejar ações. Por isso, a Auditoria validou a resposta ao item 2.2.b.

[11] Guia de PDTI do SISP – Versão 2.0 beta – Brasília, 2015.

4.11. Questão: **O processo de planejamento de TI prevê o apoio do comitê de TI.** (Item: **2.2.c.**)

4.11.1. Resposta da Instituição: **Prática adotada: integral**

4.11.2. Solicitação de comprovação: Informações sobre como é feito o PDTIC e quem tem participação no processo (SA 031/2015).

4.11.3. **Resposta NTIC** (Memorando 043/2015):

Como órgão vinculado à Secretaria de Logística e Tecnologia da Informação - SLTI do Ministério do Planejamento, Orçamento e Gestão, a UNIPAMPA por meio do NTIC segue as orientações daquele órgão que, no Guia de Elaboração de PDTI, define as regras para elaboração do PDTI da organização.

Na UNIPAMPA, o processo deve envolver a autoridade máxima da instituição, no caso a Reitora, que define as premissas e diretrizes gerais e posteriormente aprova o PDTI. Complementarmente, o CGTIC tem a função e o poder de priorizar as ações e dirigir o alinhamento dessas e dos investimentos com o planejamento estratégico da organização, no âmbito de TIC, conforme delegação do órgão colegiado máximo (CONSUNI). Portanto, o CGTIC, com a sua atual composição, é empoderado para estes fins pelo órgão máximo que representa a materialização da gestão democrática preconizada pelo Art. 56 da LDB, tendo a sua legitimidade para deliberações garantida pela sua composição com mais de 70% docentes, sendo os seus representantes sejam escolhidos pelos próprios pares (sem prejuízo, é claro, da participação dos integrantes do segmento executivo do binômio). Logo, ao NTIC, como órgão executivo, compete a execução das políticas, e a gestão da universidade devem caber a órgãos individuais. Por fim, a Equipe de Elaboração do PDTI deve possuir representantes das áreas finalísticas e de TI e tem a função de executar grande parte da elaboração do PDTI (7).

Assim sendo, é possível perceber que a UNIPAMPA atua em consonância, tanto com o que a SESU/MEC (8) preconiza, como em relação aos princípios propostos pela STLI.

(7) Guia de Elaboração de PDTI, SISP, 2012, pág. 20.
(8) http://portal.mec.gov.br/sesu/arquivos/pdf/eries.pdf

4.11.4. **Análise da Auditoria:**

Na época de construção do PDTIC da UNIPAMPA (anterior a fevereiro de 2011), o CGTIC não estava constituído. Para elaboração do conteúdo e coordenação do processo, foi designada Equipe de Elaboração do PDTIC, indicada pelo então Diretor do NTIC. Em abril de 2011, foi publicada a Portaria nº 855, designando os primeiros integrantes do Conselho Gestor de TIC da UNIPAMPA.

Através do Memorando 043/2015 foi explicitada a forma de participação do CGTIC no processo de Planejamento de TIC. Além disso, o apoio do Comitê no processo de Planejamento de TIC também foi explicitado em reunião do CGTIC, o que pode ser comprovado na Ata nº 8. Por esses motivos, a Auditoria validou a resposta ao item 2.2.c.

4.12. Questão: **A organização possui plano de TI vigente, formalmente instituído pelo seu dirigente máximo.** (Item: **2.2.e.**)

4.12.1. Resposta da Instituição: **Prática adotada: integral**

4.12.2. **Análise da Auditoria:**

De acordo com o Guia de PDTI do SISP, "o Planejamento de TI deve ser materializado em um documento escrito, publicado e divulgado no âmbito da organização, abrangendo ambientes interno e externo, relativos à área de TI".

O Planejamento de TIC da UNIPAMPA foi consolidado através do PDTIC, datado de fevereiro de 2011, e com validade de 2011 a 2015. O documento foi publicado no site do NTIC, onde está acessível interna e externamente. Sendo assim, a UNIPAMPA está de acordo com o que recomenda o SISP, por isso, a Auditoria validou a resposta ao item 2.2.e.

4.13. Questão: **O plano de TI vigente contempla objetivos, indicadores e metas para a TI, com os objetivos explicitamente alinhados aos objetivos de negócio constantes do plano estratégico institucional.** (Item: **2.2.f.**)

4.13.1. Resposta da Instituição: **Prática adotada: integral**

4.13.2. Solicitação de comprovação: Alinhamento entre os objetivos do PDTIC vigente aos objetivos de negócio constantes do PDI (SA 031/2015).

4.13.3. **Resposta NTIC** (Memorando 043/2015):

Considerando sobretudo a missão da universidade em promover educação superior de qualidade por meio da integração entre ensino, pesquisa e extensão, e tendo como visão a busca em constituir-se como instituição acadêmica de reconhecida excelência, as ações do NTIC basearam-se nestas premissas para composição das metas, conforme página 31 do PDTIC vigente.

Os objetivos gerais alinhados ao PDI que norteiam as decisões e ações de TI no âmbito da universidade são:

- Aprimorar orientações para clientes;
- Estabelecer a continuidade e disponibilidade de serviços;
- Obter informações confiáveis e úteis para o processo de decisões estratégicas;
- Prover um retorno de investimento adequado para os investimentos de TI;
- Gerenciar os riscos de negócios relacionados a TI.

Ainda, como aprimoramento interno, são elencados os seguintes objetivos gerais:

- Conformidade interna e externa;
- Estabelecer a continuidade e disponibilidade de serviços;
- Obter informações confiáveis e úteis para o processo de decisões estratégicas.

A partir destes objetivos gerais foram definidos os respectivos objetivos específicos e indicadores de forma que atendesse, considerando a situação apresentada à época, as expectativas da comunidade acadêmica.

4.13.4. **Análise da Auditoria:**

De acordo com o Guia de PDTI do SISP, é fundamental que o PDTI proporcione o alinhamento das soluções de TI às metas do negócio e às necessidades da organização, pois assim o planejamento de TI complementa o planejamento estratégico da organização. A área de TI deve possuir estratégias que promovam ações estruturantes para suportar as metas e objetivos definidos no Planejamento Estratégico do Órgão.

O PDTIC vigente estabeleceu 10 objetivos gerais e 25 objetivos específicos para a TIC, alinhados à missão da Instituição, porém não definiu explicitamente como esses objetivos contribuirão para o alcance dos objetivos estratégicos descritos no Planejamento Estratégico da UNIPAMPA.

Levando-se em consideração o PDI vigente à época da elaboração do PDTIC, válido para o período de 2009 a 2013, verificou-se que está dividido em Objetivos, Estratégias e Metas para cada política da Instituição – Política de Ensino, Política de Pesquisa, Política de Extensão, Política de Assistência Estudantil, Políticas de Gestão, Política de Gestão de Pessoal, Política de Planejamento e Avaliação, Política de Comunicação Social, totalizando 31 objetivos.

O Planejamento Estratégico atual da Instituição, válido para o período de 2014 a 2018, possui 27 objetivos estratégicos, estruturados em 4 eixos, os quais "especificam as ações a serem realizadas nos próximos cinco anos de forma a realizar o Perfil Institucional anunciado" (PDI UNIPAMPA, página 19).

Sendo assim, não foi observado alinhamento explícito com os objetivos de negócio constantes do PDI. Destaca-se também a falta de alinhamento em relação ao período de execução dos Planejamentos, visto que o atual PDTIC é válido de 2011 a 2015, elaborado com base no PDI de 2009 a 2013. O atual PDI da Instituição é de 2014 a 2018 e o PDTIC só será atualizado em 2016.

Esse descompasso pode acarretar dificuldades no acompanhamento da execução e do alcance das metas, principalmente se for observado o alinhamento mais explícito entre os objetivos do Planejamento Estratégico Institucional e do Plano de TIC.

Por todo o exposto acima, a Auditoria não validou a resposta ao item 2.2.f e considera a prática como adotada parcialmente.

4.14. Questão: **A execução do plano de TI vigente é acompanhada periodicamente quanto ao alcance das metas estabelecidas, para correção de desvios.** (Item: **2.2.h.**)

4.14.1. Resposta da Instituição: **Prática adotada: integral**

4.14.2. Solicitação de comprovação: Atual situação de realização de metas do PDTI (SA 031/2015) e mensuração do alcance atual de realização de metas do PDTI (SA 053/2015).

4.14.3. Resposta NTIC:

Memorando 043/2015 – Resposta à SA 031/2015:

O NTIC adota desde 2013 o método de gestão PDCA para controle e melhoria contínua de processos e serviços oferecidos ao NTIC. Esta metodologia é aplicada no planejamento trimestral entre a direção do núcleo e coordenadorias, de forma a mensurar o alcance das metas estabelecidas, corrigindo possíveis desvios. Portanto, o estágio atual das condições de TIC na UNIPAMPA é resultado deste processo interativo, fruto da aplicação periódica dos conceitos de PDCA, os quais justificam os necessários ajustes que foram realizados em parte das ações previstas no PDTIC aprovado em 2011.

Memorando 062/2015 – Resposta à SA 053/2015:

Em resposta à Solicitação de Auditoria nº 53/2015, apresentamos no **Anexo 1** a situação atual das metas estipuladas no Plano Diretor de TIC vigente, o qual serviu de referencial de ações passíveis de serem executadas ao longo do seu período de vigência.

Cabe ressalvar a natureza inovadora deste plano diretor de TI, o qual foi o primeiro da instituição e um dos primeiros produzidos nas universidades federais brasileiras. Como é comum em ações pioneiras, este plano, apesar de cumprir com o seu papel de nortear as ações administrativas da instituição no contexto de TICs, mostrou-se parcialmente inexequível, tanto do ponto de vista da quantidade excessiva de ações previstas como pela presença de diversas metas inatingíveis, se considerados os recursos disponíveis para o setor durante este período de maturação das equipes e de desafios naturais de uma instituição de ensino superior federal em implantação.

Salientamos, porém, que a análise atual das metas fundamenta-se em uma nova metodologia, conforme abordado no Memorando Nº 43/2015-NTIC em resposta a Solicitação de Auditoria 31/2015, cujo detalhamento será apresentado no novo Plano Diretor de TIC, com previsão de publicação para o segundo semestre de 2015. Trata-se, sobretudo, do alinhamento com o Plano de Desenvolvimento Institucional (PDI) 2014-2018 da UNIPAMPA, com objetivos otimizados e permitindo revisões de metas em menores intervalos de tempo, além de indicadores com maior eficiência de monitoramento.

Quanto a análise das metas no **Anexo 1**, esclarecemos que as situações na qual se encontram como parcialmente atingidas, atingidas ou postergadas, foram reavaliadas conforme atual metodologia, considerando os recursos disponíveis e ações que interferem direta ou indiretamente nos objetivos, mencionadas na coluna Ações Relacionadas, além do método PDCA com reavaliação inclusive das próprias metas estipuladas.

4.14.4. Análise da Auditoria:

De acordo com o e-Ping 2015[12], PDCA (Planejar-Executar-Verificar-Agir) é uma ferramenta de gestão da qualidade com foco na melhoria contínua de processos, onde cada passo corresponde a:

- Planejar: estabelecer os processos necessários para entregar resultados de acordo com os objetivos e as metas projetadas;
- Executar: implementar o plano, executar o processo e coletar dados para mapeamento e análise dos passos seguintes;
- Verificar: confrontar o resultado alcançado no passo anterior com os objetivos e as metas estabelecidas no primeiro passo, para determinar quaisquer diferenças;
- Agir: tomar ações corretivas sobre as diferenças significativas entre os resultados reais e os planejados, analisando as diferenças para determinar suas causas.

A questão do item 2.2.h. pode ser encaixada no ciclo PDCA, tratando-se de questionamento sobre os passos “verificar” e “agir” do plano de TIC vigente. Após análise das respostas contidas nos Memorandos e do Anexo 1, foi possível comprovar que a execução do plano de TIC está sendo monitorada, através do acompanhamento do alcance das metas estabelecidas no PDTIC 2011-2015.

O Plano de TIC vigente é composto por 25 objetivos específicos, onde cada um possui uma ou mais metas macro. No Anexo apresentado à Auditoria, cada uma dessas metas possui um indicador que, por sua vez, está relacionado a metas anuais de alcance. Há também a informação de “Situação atual” e “Ações relacionadas”, que são as colunas que traduzem efetivamente o

[12] Padrões de Interoperabilidade de Governo Eletrônico – Documento de Referência da e-Ping – versão 2015.

acompanhamento que está sendo feito e as ações pretendidas para alcançar as metas ainda não atingidas, como mostrado a seguir:

Figura 3 – Acompanhamento de metas

OBJETIVO	META	INDICADOR	METAS ANUAIS					SITUAÇÃO ATUAL	AÇÕES RELACIONADAS
			2011	2012	2013	2014	2015		
Adquirir e manter uma infraestrutura de TIC integrada e padronizada.	MANTER INFRAESTRUTURA DE TECNOLOGIA	Plataformas não alinhadas		60%	40%	20%	10%	Parcialmente atingido	Projeto datacenter principal e datacenter de contingência.
		Processos sustentados por infra obsoleta		60%	40%	20%	10%	Parcialmente atingido	Projeto datacenter principal e datacenter de contingência.
	RECURSOS DE TIC	Satisfação com fornecedores de TIC	60%	70%	80%	90%	95%	Atingido	Método PDCA, levando a novas contratações quando constatado o nível de serviço aquém do necessário.
Adquirir e manter sistemas aplicativos integrados e padronizados	PLANO DE INFRA-ESTRUTURA TECNOLÓGICA	Frequência de revisão atualização do planejamento		1	1	1	1	Atingido	Reavaliado conforme método PDCA.
		Quantidade de desvios do plano de infraestrutura		10	5	3	2	Atingido	Reavaliado conforme método PDCA.
Assegurar apropriado uso e a performance das soluções de aplicativos e de tecnologia.	OPERAÇÃO E USO	Aplicações com treinamento de SO e de Usuário	10	12	14	16	18	Atingido	Reavaliado conforme método PDCA.
		Satisfação com treinamentos e material	75%	80%	90%	95%	97%	Postergado	Instituir mecanismo de survey para quantificar a satisfação.
	TREINAR USUÁRIOS	Chamadas por falta de treinamento	150	100	70	50	20	Parcialmente atingido	Qualificar ações de capacitação por EAD em parceria com NUDEPE.
Adquirir e manter habilidades de TIC	RECURSOS DE TI	Eficácia no processo de compras	15%	20%	25%	30%	35%	Atingido	Reavaliado conforme método PDCA.
		% do Plano de Capacitação Atingido	60%	65%	70%	90%	100%	Parcialmente atingido	Qualificar plano de capacitações anual em parceria com NUDEPE com foco nas atribuições e responsabilidades as equipes.
		Nível de Satisfação com interações em TI	60%	75%	80%	90%	95%	Postergado	Instituir mecanismo de survey para quantificar a satisfação

FONTE: Adaptado do Anexo recebido

Sendo assim, a resposta ao item 2.2.h foi validada pela Auditoria.

4.15. Questão: **O plano de TI vigente vincula as ações (atividades e projetos) a indicadores e metas de negócio.** (Item: **2.2.i.**)

4.15.1. Resposta da Instituição: **Prática adotada: integral**

4.15.2. Solicitação de comprovação: Vinculação das ações do PDTI vigente a indicadores e metas de negócio (SA 031/2015).

4.15.3. **Resposta NTIC** (Memorando 043/2015):

O PDTI explicita os indicadores e metas por meio de seus objetivos específicos, com texto introdutório que detalha ações que envolvem o alcance das metas anuais estipuladas. As metas anuais compreendem o período de 2011 a 2015, entretanto, as revisões destas ações impactam diretamente no atingimento das metas. Espera-se que com a revisão do PDTI, as ações, assim como o resultado de reuniões e tratativas recentes com a alta gestão sejam sintetizados em objetivos específicos, com indicadores e metas proporcionais à atual evolução da instituição, considerando também o a metodologias adotada para a revisão do planejamento, em menor período de tempo, conforme mencionado anteriormente. Estes complementarão as ações e metas, no âmbito de TIC, que já estão formalizadas no atual PDI da UNIPAMPA.

4.15.4. **Análise da Auditoria:**

As ações do plano de TIC vigente estão descritas brevemente após cada objetivo específico, traduzindo como será a atividade desenvolvida para alcançar a meta relacionada. Os objetivos específicos estão alocados em quatro perspectivas e estão acompanhados por metas e indicadores. Sendo assim, pode-se afirmar que o plano de TIC vincula ações a indicadores e metas,

como pode ser verificado a partir da página 31 do PDTIC, validando a resposta ao item 2.2.i. Ressalta-se, porém, que, diferentemente do que está relatado no Memorando 043/2015, o atual PDI da UNIPAMPA não possui metas no âmbito de TIC.

4.16. Questão**: A organização realiza avaliação periódica de segurança da informação.** (Item: **1.7.d.**)

4.16.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.16.2. Solicitação de comprovação: Relatório de incidentes ou eventos relacionados à segurança da informação e o tratamento dado a cada um deles (2013-2015), ou justificativa, caso permaneça a situação de prática não adotada (SA 044/2015).

4.16.3. Resposta NTIC (Memorando 055/2015):

As atribuições sob responsabilidade da Coordenadoria de Segurança da Informação (CSI) do NTIC abrangem avaliações periódicas que ocorrem com base em determinados elementos. Um deles é o Relatório Mensal de Incidentes enviado pelo Centro de Atendimento de Incidentes de Segurança (CAIS) da RNP, grupo de resposta da rede acadêmica brasileira, que detecta, resolve e previne incidentes de segurança (1).

Concomitantemente, é realizada, por amostragem (periodicidade mensal) ou por solicitação das equipes responsáveis pelos serviços, uma análise de vulnerabilidades existentes nos serviços ativos da instituição. Quando encontradas vulnerabilidades de nível alto, os responsáveis pela instância do serviço são notificados para correção dos problemas.

Além desta atividade, periodicamente é realizado, juntamente com a direção do NTIC, o planejamento trimestral da respectiva Coordenadoria, com o objetivo de propor soluções para aperfeiçoamento de processos e procedimentos relacionados à segurança da informação.

Atualmente, parte das atribuições no contexto de segurança da informação está em processo de migração para um novo modelo, decorrente da criação da Estrutura de Segurança da Informação e Comunicação (ESIC), a qual concentrará o registro dos incidentes de segurança que ocorrerem no âmbito da UNIPAMPA, conforme o Art. 1º da Resolução 83/2014 do CONSUNI (2). Cabe esclarecer que a ESIC está em formação, e por alterar a estrutura organizacional do NTIC, deve ocorrer por meio de Portaria (3), com publicação prevista ainda para o corrente semestre.

Portanto, embora o NTIC realize avaliações de segurança da informação por meio de sua Coordenadoria específica, o plano para qualificação deste serviço está em andamento com a composição da ESIC.

(1) http://www.rnp.br/servicos/seguranca

4.16.4. Análise da Auditoria:

Após análise do Memorando 055/2015, concluímos que existem três ações no âmbito de avaliação de segurança da informação:

1. Avaliações periódicas, sob responsabilidade da CSI, com base em determinados elementos, como por exemplo o Relatório Mensal de Incidentes enviado pelo CAIS da RNP.
2. Análise mensal de vulnerabilidades nos serviços ativos da Instituição, realizada por amostragem ou por solicitação das equipes responsáveis pelos serviços.
3. Planejamento trimestral da CSI, juntamente com a direção do NTIC, com o objetivo de propor soluções para aperfeiçoamento de processos e procedimentos relacionados à segurança da informação.

Sendo assim, pode-se considerar que a Instituição saiu da situação de prática não adotada para prática adotada integralmente para o item 1.7.d. Salienta-se, porém, a importância da formalização da ESIC, que concentrará o registro dos incidentes de segurança no âmbito da UNIPAMPA, conforme o Artigo 1º da Resolução nº 83/2014 do CONSUNI.

4.17. Questão: **A organização dispõe de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.** (Item: **5.4.a.**)

4.17.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.17.2. Solicitação de comprovação: Política de segurança da informação normatizada e formalizada, ou justificativa, caso permaneça a situação de prática não adotada (SA 044/2015).

4.17.3. **Resposta NTIC** (Memorando 055/2015):

> Uma das atribuições da Estrutura de Segurança da Informação e Comunicação da UNIPAMPA será a criação da Política de Segurança da Informação e Comunicações (POSIC), conforme art. 6º da resolução que cria a ESIC. Ela ainda será responsável por avaliar, revisar e analisar criticamente esta política e suas normas complementares, visando a sua aderência aos objetivos institucionais da UNIPAMPA e às legislações vigentes. Por outro lado, cabe destacar que já existe uma proposta de POSIC, construída a partir de um GT de segurança que trabalhou no tema, nos últimos anos, com representação de diferentes setores da instituição. Esta proposta será apresentada ao órgão máximo da ESIC, o Comitê de Segurança da Informação e Comunuicações (CSIC), para apreciação, inclusão de modificações pertinente e aprovação. Cabe destacar que, conforme estabelecido na resolução de criação da ESIC, este Comitê possui caráter consultivo, propositivo e de apoio, estando vinculado diretamente à Reitoria da Universidade, sem subordinação hierárquica às demais pró-reitorias e direções de Campus.

4.17.4. **Análise da Auditoria:**

De acordo com o Guia ao Gestor em SIC[13], a POSIC formalizada, institucionalizada e divulgada, resulta na promoção de uma cultura de SIC, por intermédio de iniciativas institucionais de sensibilização, conscientização, capacitação e especialização.

Na Instituição, a POSIC ainda não está formalmente instituída, apesar de haver uma proposta dessa Política, como exposto no Memorando 055/2015. Sendo assim, a prática do item 5.4.a. continua não sendo adotada.

4.18. Questão: **A organização dispõe de comitê de segurança da informação formalmente instituído, responsável por formular e conduzir diretrizes para a segurança da informação corporativa, composto por representantes de áreas relevantes da organização.** (Item: **5.4.b.**)

4.18.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

[13] Guia de Orientações ao Gestor em Segurança da Informação e Comunicações – DSIC. Versão 01 – Fev./2014.

4.18.2. Solicitação de comprovação: Composição e data em que foi formalmente instituído o Comitê de Segurança da Informação, ou justificativa, caso permaneça a situação de prática não adotada (SA 044/2015).

4.18.3. **Resposta NTIC** (Memorando 055/2015):

O Comitê de Segurança da Informação e Comunicações (CSIC) está previsto na Estrutura de Segurança da Informação e Comunicação da UNIPAMPA (ESIC), conforme art. 2º da Resolução 83/2014. Conforme já mencionado, a portaria para designação dos membros desta nova estrutura será publicada em breve, na sequência da formalização da ESIC dentro da estrutura da UNIPAMPA.

Deverão compor o CSIC:

I. Vice-Reitor;

II. Gestor de Segurança da Informação e Comunicações;

III. Diretor do Núcleo de Tecnologia da Informação e Comunicações;

IV. Responsável pela consultoria jurídica; V. Pró-Reitor de Gestão de Pessoal;

VI. Pró-Reitor de Planejamento ou representante de infraestrutura;

VII. um representante do Comitê Gestor de Tecnologia da Informação e Comunicações (CGTIC).

4.18.4. **Análise da Auditoria:**

A Norma Complementar Nº 03/DSIC/GSIPR recomenda:

> 5.3.7.3 Instituir o Comitê de Segurança da Informação e Comunicações do órgão ou entidade da APF com as seguintes responsabilidades:
>
> a) Assessorar na implementação das ações de segurança da informação e comunicações no órgão ou entidade da APF;
>
> b) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações; e
>
> c) Propor Normas e Procedimentos internos relativos à segurança da informação e comunicações, em conformidade com as legislações existentes sobre o tema.

A Resolução nº 083/2014 prevê, na estrutura da ESIC, o Comitê de Segurança da Informação e Comunicações – CSIC, que deverá ser composto por representantes de áreas relevantes da Instituição. Porém, como a ESIC ainda não foi formalmente instituída, o CSIC não existe em nível Institucional. Sendo assim, a prática do item 5.4.b. continua não sendo adotada.

4.19. Questão: **A organização dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.** (Item: **5.4.d.**)

4.19.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.19.2. **Análise da Auditoria:**

Essa política está formalmente instituída através da Norma de Uso de Credenciais de Acesso, além de ser uma das diretrizes da ESIC.

Na Resolução nº 83/2014, na Seção IV – Do Controle de Acesso, consta:

> Art. 18 Todo acesso à informação que não seja de domínio público se dá através de mecanismos de identificação e controle de acesso.

§1º Qualquer mudança funcional implica na revisão dos direitos de acesso à informação;

§2º O usuário deve ter pleno conhecimento das diretrizes, responsabilidades, limitações e penalidades relacionadas à utilização dos recursos de informação, inclusive por ocasião da mudança de atividades.

Art. 19 O ambiente que contenha ativos de informação deve ser protegido de acordo com sua severidade.

Art. 20 No gerenciamento de operações e comunicações deve-se garantir a operação segura e correta dos recursos de processamento da informação e das comunicações.

Como previsto no Artigo 8º da Resolução, para cada uma das diretrizes devem ser elaboradas normas táticas específicas, manuais e procedimentos. Nesse sentido, foi criada a Norma de Uso de Credenciais de Acesso, com o objetivo de "estabelecer critérios de responsabilidade sobre o uso de dispositivos de identificação e ou senhas, e os procedimentos de segurança para gerenciamento de senhas para acesso aos diversos ativos de TIC, no âmbito da UNIPAMPA". Sendo assim, a prática do item 5.4.d pode ser considerada como adotada integralmente.

4.20. Questão: **A organização dispõe de política de cópias de segurança (backup) formalmente instituída, como norma de cumprimento obrigatório.** (Item: **5.4.e.**)

4.20.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.20.2. Solicitação de comprovação: Política de cópias de segurança (backup) normatizada e formalizada, ou justificativa, caso permaneça a situação de prática para não adotada (SA 044/2015).

4.20.3. **Resposta NTIC** (Memorando 055/2015):

A ESIC será responsável por elaborar e instituir uma política para este tipo de procedimentos no âmbito da UNIPAMPA, que poderá fazer parte da Política de Segurança da Informação e Comunicação (POSIC) a ser criado após a formalização desta nova estrutura.

Entretanto, o NTIC já realiza ações neste sentido, dispondo de um serviço de backup centralizado para realizar cópias de segurança em todas as instâncias (servidores e serviços) hospedadas nos Data Centers institucionais, sob responsabilidade do NTIC, de forma automática e periódica, com base em software livre. Além disso, é realizado um esquema complementar de backup remoto, com armazenamento de dados dos sistemas disponibilizados a partir do data center principal no data center de contingência e vice-versa. Cabe destacar que o serviço atual é resultado de um reestudo realizado sobre o procedimento de backup após o grave incidente de indisponibilidade de serviços e perda de dados ocorrido no segundo semestre de 2013.

4.20.4. **Análise da Auditoria:**

Após análise da resposta apresentada, conclui-se que a prática de cópias de segurança (backup) existe na Instituição, porém ainda não é uma política formalmente instituída, por depender da formalização da ESIC na estrutura da UNIPAMPA. Sendo assim, a prática do item 5.4.e continua não sendo adotada.

4.21. Questão: **O processo para classificação e tratamento de informações está formalmente instituído, como norma de cumprimento obrigatório.** (Item: **5.4.i.**)

4.21.1. Resposta da Instituição: **Prática adotada: parcial**

4.21.2. Solicitação de comprovação: Processo para classificação e tratamento das informações normatizado e formalizado (SA 044/2015).

4.21.3. **Resposta NTIC** (Memorando 055/2015):

O processo para classificação e tratamento de informações, na UNIPAMPA, está balizado tanto por aspectos da Lei de Acesso a Informação (1), que determina a "observância da publicidade como preceito geral e do sigilo como exceção", como pelo respeito às premissas contidas no Anexo A da 20/IN01/DSIC/GSIPR (2), o qual destaca informações pré-classificadas como sigilosas. Atualmente a UNIPAMPA não possui informações sigilosas classificadas (3) como reservadas pela autoridade máxima, após parecer da CPADS (4). Assim sendo, o NTIC restringe acesso aos dados armazenados nos sistemas de informação institucionais em consonância com estas classificações, privilegiando, sempre que possível, a viabilização de instrumentos que facilitem a busca ativa a informações que possuem tipo de acesso ostensivo, bem como fornecendo o acesso a informações específicas. As informações específicas são liberadas por meio de relatórios especializados disponibilizados por meio do sistema GURI, tanto para os setores que possuem responsabilidade sobre a fidedignidade da alimentação dos dados nos sistemas, como para a Divisão de Dados Institucionais (5) da PROPLAN, setor que concentra a responsabilidade por fornecer dados da instituição para a comunidade interna e externa da UNIPAMPA.

(1) http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm
(2) http://dsic.planalto.gov.br/documentos/NC20_Revisao01.pdf
(3) http://porteiras.r.unipampa.edu.br/portais/acessoainformacao/informacoes-classificadas
(4) Portaria 640/2014 - Gabinete da Reitora
(5) http://porteiras.r.unipampa.edu.br/portais/proplan/dados-institucionais/

4.21.4. **Análise da Auditoria:**

Pelo exposto no Memorando, conclui-se que o processo para classificação e tratamento de informações está balizado pela Lei de Acesso à Informação – LAI (Lei 12.527/2011) e pela Norma Complementar Nº 20/IN01/DSIC/GSIPR, ambas a serem observadas pela Administração Pública Federal, além de conter previsão na Resolução nº 83/2014:

> Art. 13 A classificação e o tratamento de informação são:
> I. norteados pela legislação específica que disponha sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal (APF);
> II. implementados e mantidos em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada informação custodiada ou de propriedade da UNIPAMPA ao longo do seu ciclo de vida.

A CPADS – Comissão Permanente de Avaliação de Documentos Sigilosos, mencionada no Memorando, foi constituída através da Portaria 640/2014 e tem como objetivo atender demandas específicas que necessitam de um parecer acerca da classificação de informações. O trabalho da Comissão é apenas consultivo. Qualquer setor/unidade da instituição pode solicitar um parecer à CPADS, no entanto, a efetiva classificação da informação só pode ser deliberada pela autoridade competente da Universidade, conforme Art. 27 da Lei 12.527/2011.

Sendo assim, a Auditoria considera que a prática do item 5.4.i passou a ser adotada integralmente.

4.22. Questão: **A organização implementa controles para garantir a proteção adequada ao grau de confidencialidade de cada classe de informação.** (Item: **5.4.j.**)

4.22.1. Resposta da Instituição: **Prática adotada: integral**

4.22.2. Solicitação de comprovação: Controles implementados para proteger cada classe de informação (SA 044/2015).

4.22.3. **Resposta NTIC** (Memorando 055/2015):

Todos os sistemas de informação da UNIPAMPA possuem gestão de perfis de acesso a dados e funcionalidades. Os servidores são enquadrados em perfis individuais ou de grupo em conformidade com as funções que desempenha na instituição, a partir de solicitações da sua chefia ou superior hierárquico por meio do sistema de chamados (1), o que torna o processo auditável quando combinado com as regras de uso de credenciais institucionais (2) e mecanismos de registro de logs de acesso. Além disso, novos relatórios, com acesso a dados sigilosos, só são desenvolvidos e liberados para os setores que possuem responsabilidade para manipulá-los.

(1) https://chamados.unipampa.edu.br
(2) http://ntic.unipampa.edu.br/files/2015/01/NormaDeUsoDeCredenciais.pdf

4.22.4. **Análise da Auditoria:**

A UNIPAMPA não possui informações classificadas em grau de sigilo, por isso, as informações são consideradas do tipo Ostensivas e divulgadas através de Transparência Ativa ou Transparência Passiva, conforme Decreto 7.724/2012:

> DA TRANSPARÊNCIA ATIVA
> [...]
> Art. 8º Os sítios na Internet dos órgãos e entidades deverão, em cumprimento às normas estabelecidas pelo Ministério do Planejamento, Orçamento e Gestão, atender aos seguintes requisitos, entre outros:
> I - conter formulário para pedido de acesso à informação;
> II - conter ferramenta de pesquisa de conteúdo que permita o acesso à informação de forma objetiva, transparente, clara e em linguagem de fácil compreensão;
> III - possibilitar gravação de relatórios em diversos formatos eletrônicos, inclusive abertos e não proprietários, tais como planilhas e texto, de modo a facilitar a análise das informações;
> IV - possibilitar acesso automatizado por sistemas externos em formatos abertos, estruturados e legíveis por máquina;
> V - divulgar em detalhes os formatos utilizados para estruturação da informação;
> VI - garantir autenticidade e integridade das informações disponíveis para acesso;
> VII - indicar instruções que permitam ao requerente comunicar-se, por via eletrônica ou telefônica, com o órgão ou entidade; e
> VIII - garantir a acessibilidade de conteúdo para pessoas com deficiência.
> DA TRANSPARÊNCIA PASSIVA
> Do Serviço de Informação ao Cidadão
> Art. 9º Os órgãos e entidades deverão criar Serviço de Informações ao Cidadão - SIC, com o objetivo de:

I - atender e orientar o público quanto ao acesso à informação;

II - informar sobre a tramitação de documentos nas unidades; e

III - receber e registrar pedidos de acesso à informação.

De acordo com o Memorando 055/2015 e com o Decreto nº 7.724, o acesso às informações ostensivas deve ser viabilizado através do site da Instituição, com todos os pré-requisitos listados no artigo 8º, e as informações que não estão divulgadas devem ser disponibilizadas mediante solicitação. Essas práticas já vêm sendo adotadas na Instituição, que implementa controles para garantir a proteção adequada a cada classe de informação, por isso a resposta ao item 5.4.j foi validada pela Auditoria.

4.23. Questão: **A organização executa processo de gestão de riscos de segurança da informação.** (Item: **5.4.k.**)

4.23.1. Resposta da Instituição: **Prática adotada: integral**

4.23.2. Solicitação de comprovação: Plano de Gestão de Riscos (SA 044/2015).

4.23.3. **Resposta NTIC** (Memorando 055/2015):

Consta entre os princípios e diretrizes da Norma Complementar 04/IN01/DSIC/GSI/PR (1), os processos de Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC deverão considerar, prioritariamente, os objetivos estratégicos, os processos, os requisitos legais e a estrutura do órgão ou entidade da APF, direta e indireta, além de estarem alinhadas à respectiva Política de Segurança da Informação e Comunicações do órgão ou entidade. Portanto, é inegável que a formalização, por completo, deste processo é dependente de uma ação anterior, a da formalização da POSIC.

Por outro lado, independentemente desta formalização, os princípios que amparam a gestão de risco podem ser igualmente aplicados sobre os ativos de informação a partir de uma análise preliminar realizada pelas equipes responsáveis pela disponibilidade dos serviços. Assim sendo, considerando o cenário atual de ausência da POSIC, a gestão de riscos tem sido responsabilidade da Coordenadoria de Segurança da Informação do NTIC, a qual tem por atribuição identificar, analisar e tratar os possíveis riscos de segurança nos diferentes ativos de informação gerenciados pelo NTIC. Neste sentido, várias são as ações executadas pelo NTIC para reduzir as vulnerabilidades existentes e evitar incidentes que possam comprometer dados institucionais. Como exemplo podem ser destacados: (i) Serviços de cópias de segurança (backups); (ii) Configuração dos firewalls(2) institucionais para prevenção de ataques; (iii) Ajuste periódico no nível de segurança de senhas e mecanismos complementares de identificação associados às credenciais de acesso.

Estas ações são baseadas em normas sobre o assunto, como a NBR 31000 e NBR 27005, e difundidas pela Escola Superior de Redes, órgão que por meio da Rede Nacional de Pesquisa (RNP) oferece capacitações na área para qualificação destes serviços. Capacitações que fazem parte do Plano de Capacitação Anual do NTIC enviado ao NUDEPE em Julho de 2014 (3) em conformidade com o Art. 21 da Resolução No. 24 do CONSUNI (4)

(1) http://dsic.planalto.gov.br/documentos/nc_04_grsic.pdf
(2) Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
(3) Memorando No. 69/2014 NTIC/UNIPAMPA
(4) http://porteiras.r.unipampa.edu.br/portais/progesp/files/2010/08/Res.-24_2010-Programa-de-Capacita%C3%A7%C3%A3o.pdf

4.23.4. **Análise da Auditoria:**

De acordo com a Norma Complementar 04/IN01/DSIC/GSI/PR, o processo de Gestão de Gestão de Riscos de SIC é composto por:

1. Definições preliminares

2. Análise/avaliação dos riscos
3. Plano de Tratamento dos riscos
4. Aceitação dos riscos
5. Implementação do Plano de Tratamento dos Riscos
6. Monitoração e Análise crítica

No PDTIC da Instituição consta que foi realizado um diagnóstico, que resultou em duas fontes de informações a serem consideradas no Plano de Gestão de Riscos:

a) principais incidentes ocorridos ao longo dos primeiros anos de implantação da Instituição;

b) mapa de riscos que foram identificados e incluídos no PDTIC.

Foi então apresentada Análise de Incidentes, bem como Plano de Ação para Mitigação de Incidentes e o Mapa de Risco e Mapa de Risco por Projeto.

A partir da resposta do Memorando 055/2015 e com base na Norma Complementar 04, pode se considerar que a Instituição executa processo de gestão de riscos de segurança da informação, formalizada nas páginas 144 a 155 do PDTIC. Sendo assim, a Auditoria validou a resposta ao item 5.4.k.

Ressalta-se, porém, que esse documento necessita de atualização para adequação à realidade atual da Instituição.

4.24. Questão: **A organização executa processo de monitoramento do uso dos recursos de TI, com objetivo de detectar atividades não autorizadas.** (Item: **5.4.o.**)

4.24.1. Resposta da Instituição: **Prática adotada: integral**

4.24.2. Solicitação de comprovação: Relatórios de incidentes/eventos de acesso não autorizado em sistemas ou na rede da UNIPAMPA (SA 044/2015).

4.24.3. **Resposta NTIC** (Memorando 055/2015):

Embora não haja registros recentes de acesso não autorizado a sistemas ou a rede da UNIPAMPA, exceto relatos de e-mails recebidos pelos membros da comunidade caracterizados como SPAM ou Phishing, registrados no CAIS/RNP, estão implementadas funcionalidades preventivas e reativas para o caso de suspeita de ocorrência de acesso não autorizado. Cabe a Coordenadoria de Segurança da Informação do NTIC monitorar estes serviços, no qual destacamos os mais relevantes:

- Servidor de Logs central: esse serviço visa armazenar os logs e eventos dos servidores e serviços para futuras trilhas de auditoria em caso de necessidade;
- Bloqueio automático da troca de senha de um usuário caso o mesmo erre 3 vezes consecutivas na troca de senhas. Nesse caso um e-mail é enviado para o usuário e para a CSI informando o ocorrido;
- Bloqueio do usuário por 5 minutos caso o usuário tente acessar o SIE e erre a senha por 3 vezes consecutivas;
- Bloqueio de acesso de conexões externas a partir de endereços de origem identificados como possíveis ameaças a partir de diferente técnicas incluindo blacklists externas que listam endereços denunciados em âmbito mundial ou regional com fonte de atividades suspeitas, blacklists internas dos sistemas de gestão de conteúdo usados nos portais institucionais para conter tentativas de negação de serviço e outras técnicas de intrusão, bem como mecanismos IDS (instrusion detection system) disponibilizados pelo fabricante dos firewalls implantados na UNIPAMPA e que incorporam bases atualizáveis com assinaturas de diferentes tipos de ataques.

4.24.4. Análise da Auditoria:

As ferramentas utilizadas pela CSI, expostas no Memorando 055/2015, são práticas que demonstram que é executado processo para monitoramento do uso dos recursos de TIC, validando a resposta ao item 5.4.o.

4.25. Questão: **A organização possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais, formalmente instituída.** (Item: **5.4.s.**)

4.25.1. Resposta da Instituição: **Prática adotada: integral**

4.25.2. Solicitação de comprovação: Composição e data em que foi formalmente instituída Equipe de Tratamento, e Resposta a Incidentes de Segurança em Redes Computacionais (SA 044/2015).

4.25.3. Resposta NTIC (Memorando 055/2015):

Atualmente a equipe com esta atribuição está formada na Coordenadoria de Segurança da Informação do NTIC (1). Em breve esta responsabilidade deverá ser migrada para a nova Estrutura de Segurança da Informação e Comunicação da UNIPAMPA.

(1) http://ntic.unipampa.edu.br/coordenacoes/csi/

4.25.4. Análise da Auditoria:

O Guia ao Gestor em SIC traz alguns direcionamentos sobre a Equipe de Tratamento e Respostas a Incidentes em Redes Computacionais – ETIR:

> 2.2.2.1. Criação da ETIR
>
> Para a criação de uma ETIR, a organização deve possuir a competência formal para administração total ou parcial da infraestrutura da rede de computadores da organização. Uma vez estabelecida a competência, com o apoio e chancela da Alta Administração, deve ser publicado, alinhado com a POSIC da organização, o documento de constituição da ETIR.
>
> Neste sentido, cumpre evidenciar os requisitos mínimos para a instituição da ETIR:
>
> • Definir sua missão - propósito e estrutura das atividades desenvolvidas. A definição da missão fornecerá a linha base para as atividades a serem desenvolvidas pela Equipe;
>
> • Público-alvo - usuários da organização e relacionamentos externos;
>
> • Estrutura proporcional à complexidade da organização;
>
> • Modelo de implementação;
>
> • Nível de autonomia; e
>
> • Serviços que serão prestados.

Foi possível verificar que, na Coordenadoria de Segurança da Informação – CSI do NTIC, existe uma equipe que exerce as mesmas funções da ETIR, conforme explicitado no Memorando 055/2015. A CSI foi formalmente instituída na estrutura da Instituição através da Portaria nº 367, de 18 de abril de 2013. Por esse motivo, a resposta ao item 5.4.s. foi validada pela Auditoria.

4.26. Questão: **A organização realiza, de forma periódica, ações de conscientização, educação e treinamento em segurança da informação para seus colaboradores.** (Item: **5.4.t.**)

4.26.1. Resposta da Instituição: **Prática adotada: integral**

4.26.2. Solicitação de comprovação: Ações realizadas para conscientização, educação e treinamento em segurança da informação para os colaboradores (SA 044/2015).

4.26.3. **Resposta NTIC** (Memorando 055/2015):

A UNIPAMPA participa anualmente do DISI - Dia Internacional de Segurança em Informática, evento voltado a usuário final de computadores que tem como objetivo promover boas práticas relacionadas à segurança da informação. Este evento é organizado pela Rede Nacional de Pesquisa, no qual a universidade mantém vínculo permanente. Na UNIPAMPA o evento é organizado pelo NTIC, com ações de divulgação das informações repassadas pelos organizadores, inclusive palestras transmitidas pela internet sobre o tema. Este ano o evento está previsto para todo o mês de setembro (1).

Anualmente também são divulgadas as cartilhas com recomendações e dicas sobre como o usuário pode se prevenir e aumentar a sua segurança na Internet, este material é elaborado pelo Cert.br (2), Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), que é um dos serviços prestados para a comunidade Internet do Brasil pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), o braço executivo do Comitê Gestor da Internet no Brasil (CGI.br).

Ainda, por meio de vagas disponibilizadas anualmente pela Escola Superior de Redes (3), sem custo à universidade, são realizadas capacitações na área de segurança de forma a qualificar os serviços sob responsabilidade do NTIC. Estes cursos, de cunho técnico, são realizados por membros do núcleo como também pelos servidores que atuam no suporte de TI dos campi.

Por fim, cabe destacar a preocupação do DSIC com o tema, materializada na Norma Complementar 18/IN01/DSIC/GSIPR (4). Em particular, na UNIPAMPA foi feita uma atividade pioneira de sensibilização de ambientação em SIC, de 1h, com a alta gestão - reitora, vice-reitor e pró-reitores - no segundo semestre de 2014, a cargo de um docente especialista na área - Érico Amaral.

(1) https://disi.rnp.br/
(2) http://cartilha.cert.br/sobre/
(3) https://esr.rnp.br/cursos
(4) http://dsic.planalto.gov.br/documentos/nc_18_atividades_ensino.pdf

4.26.4. **Análise da Auditoria:**

De acordo com a Norma Complementar Nº 18, os Agentes Públicos deverão receber orientações em Segurança da Informação e Comunicações no período de ambientação, formação inicial ou continuada em seus órgãos ou entidades, por meio de atividades de ensino de sensibilização, conscientização, capacitação e especialização e recomenda que os órgãos e entidades da APF invistam na formação continuada dos profissionais da área de Segurança da Informação e Comunicações por meio de cursos de extensão e especialização.

Através da resposta e dos links fornecidos, foi possível verificar que a Instituição realiza, de forma periódica, ações de educação e treinamento em segurança da informação para os colaboradores da área de TI e divulga ações de conscientização para a comunidade Universitária, validando a resposta ao item 5.4.t.

4.27. Questão: **A organização realiza estudos técnicos preliminares para avaliar a viabilidade da contratação.** (Item: **5.7.a.**)

4.27.1. Resposta da Instituição: **Prática adotada: integral**

4.27.2. Contratos analisados: **10/2011 e 58/2014.**

4.27.3. Análise da Auditoria:

A contratação sem realização de estudos técnicos preliminares pode levar à contratação sem resultados capazes de atender à necessidade da Instituição, com consequente desperdício de recursos públicos.

De acordo com o Guia Prático de Contratações de TI[14], o Estudo Técnico Preliminar tem por objetivo realizar uma análise detalhada sobre a viabilidade, ou não, da demanda gerada no DOD (Documento de Oficialização da Demanda), demonstrando a viabilidade técnica e econômica da contratação.

Após análise dos processos selecionados como amostra, verificou-se que ambos possuem realização de estudos técnicos preliminares, materializados principalmente em descrições detalhadas, especificações mínimas e orçamentos dos bens e/ou serviços. Sendo assim, a resposta ao item 5.7.a. foi validada.

4.28. Questão: **A organização explicita, nos autos, as necessidades de negócio que se pretende atender com a contratação.** (Item: **5.7.b.**)

4.28.1. Resposta da Instituição: **Prática adotada: integral**

4.28.2. Contratos analisados: **10/2011 e 58/2014.**

4.28.3. Análise da Auditoria:

Após análise dos processos, verificou-se que ambos contêm explicitadas, nos autos, as necessidades de negócio a serem atendidas com as contratações, através de justificativas nos pedidos de compra. Por isso, a resposta ao item 5.7.b foi validada pela Auditoria.

4.29. Questão: **A organização explicita, nos autos, os indicadores dos benefícios de negócio que serão alcançados.** (Item: **5.7.c.**)

4.29.1. Resposta da Instituição: **Prática adotada: integral**

4.29.2. Contratos analisados: **10/2011 e 58/2014.**

4.29.3. Análise da Auditoria:

Após análise dos processos selecionados como amostra, não foram encontrados elementos que pudessem servir como indicadores dos benefícios de negócio a serem alcançados. Sendo assim, não foi possível validar a resposta ao item 5.7.c.

[14] Guia de boas práticas em contratação de Soluções de Tecnologia da Informação - Ministério do Planejamento, Orçamento e Gestão - Secretaria de Logística e Tecnologia da Informação. Brasília, setembro de 2014.

4.30. Questão: **A organização adota métricas objetivas para mensuração de resultados do contrato.** (Item: **5.7.f.**)

4.30.1. Resposta da Instituição: **Prática adotada: parcial**

4.30.2. Contratos analisados: **10/2011 e 58/2014.**

4.30.3. Análise da Auditoria:

De acordo com o Guia Prático de Contratações de TI, métrica é a identificação ou descrição da unidade de medida adotada para cada indicador de qualidade a ser observado.

Após análise dos processos selecionados, não foram encontrados parâmetros definidos como métricas objetivas para mensuração dos resultados do contrato. Por esse motivo, consideramos que a prática não é adotada na Instituição.

4.31. Questão: **A organização diferencia e define formalmente os papéis de gestor e fiscal do contrato.** (Item: **5.7.i.**)

4.31.1. Resposta da Instituição: **Prática adotada: integral**

4.31.2. Contratos analisados: **10/2011 e 58/2014.**

4.31.3. Análise da Auditoria:

De acordo com o Artigo 2º da IN 04, os seguintes papéis estão envolvidos na gestão e fiscalização dos contratos de TIC:

> V - Gestor do Contrato: servidor com atribuições gerenciais, designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual, indicado por autoridade competente;
>
> VI - Fiscal Técnico do Contrato: servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área para fiscalizar tecnicamente o contrato;
>
> VII - Fiscal Administrativo do Contrato: servidor representante da Área Administrativa, indicado pela autoridade competente dessa área para fiscalizar o contrato quanto aos aspectos administrativos;
>
> VIII - Fiscal Requisitante do Contrato: servidor representante da Área Requisitante da Solução, indicado pela autoridade competente dessa área para fiscalizar o contrato do ponto de vista funcional da Solução de Tecnologia da Informação.

Após análise dos processos selecionados como amostra, verificou-se que ambos diferenciaram e definiram formalmente os papéis de gestor e fiscal do contrato, validando a resposta ao item 5.7.i.

4.32. Questão: **A organização executa processo de planejamento das contratações de TI.** (Item: **5.8.b.**)

4.32.1. Resposta da Instituição: **Prática adotada: integral**

4.32.2. Contratos analisados: **10/2011 e 58/2014.**

4.32.3. Solicitação: comprovação de prática adotada integralmente (SA 061/2015).

4.32.4. **Resposta NTIC** (Memorando 074/2015)**:**

Todas as contratações de bens e serviços de TI são precedidas de Estudo Técnico Preliminar, em conformidade com a instrução Normativa MP/SLTI 04/2014. Nesta fase inicial ocorre a definição e especificação das necessidades de negócio e tecnológicas, e/ou dos requisitos necessários e suficientes à escolha da Solução de Tecnologia da Informação.

Um dos meios de identificação das demandas ocorre com o Documento de Oficialização de Demandas (DOD), formulário específico para este registro, que possui processo consolidado e publicado (1). O NTIC também identifica demandas entre as unidades e, sob iniciativa própria, realiza a análise de viabilidade técnica de possíveis soluções no âmbito da universidade.

Todas as informações coletadas na fase de planejamento são organizadas nos Termos de Referência destas contratações, sob responsabilidade do NTIC, respeitando o Decreto nº 5.450/05, art. 9º, inciso I.

No que se refere aos pregões em questão, as contratações foram precedidas deste estudo técnico, que no caso dos serviços continuados (Pregão 01/2011 e 35/2014) tiveram como ponto inicial a identificação da demanda pelo NTIC, iniciando então o diálogo com setores externos com o objetivo de conceber os respectivos Termos de Referência, conforme Anexo 1. As interações do NTIC com os Suportes de TI locais são fundamentais para consolidação dos requisitos para a nova contratação. Este contato ocorre durante o planejamento, com definição de prazos para retorno. [...]

(1) http://ntic.unipampa.edu.br/compras

4.32.5. **Análise da Auditoria:**

A partir da resposta e do Anexo apresentado, constatou-se que ambas as contratações selecionadas foram precedidas de processo de planejamento, validando a resposta ao item 5.8.b.

4.33. Questão: **O processo de planejamento das contratações de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.** (Item: **5.8.c.**)

4.33.1. Resposta da Instituição: **Prática adotada: integral**

4.33.2. Contratos analisados: **10/2011 e 58/2014.**

4.33.3. Solicitação: comprovação de prática adotada integralmente (SA 061/2015).

4.33.4. **Resposta NTIC** (Memorando 074/2015)**:**

As análises realizadas durante o planejamento respeitam as definições da IN 04/2014, art. 12, quanto à definição de requisitos, incluindo avaliação e definição dos recursos materiais e humanos necessários à implantação e continuidade dos serviços.

O planejamento das contratações seguem as orientações emitidas pela Pró-Reitoria de Administração, quanto às datas limites para protocolo de pedidos de compras, assim como demais orientações pertinentes. A exemplo das quantidades mínimas e máximas de cada item, que deverão ser efetivamente adquiridas após a conclusão do certame (2). Além disso, há o agrupamento de itens comuns possibilitando ampliar a margem de concorrência, superando o limite de contratação de pequeno porte, conforme art. 23 da Lei 8.666/93.

O NTIC também estipula uma data limite para recebimento dos registros de demandas, viabilizando os procedimentos de agrupamento e padronização de itens comuns. Este prazo está publicado na página própria para contratações de bens de TI (3) no site do NTIC.

(2) Perguntas Frequentes, Questionamento 1; http://porteiras.r.unipampa.edu.br/portais/cmp/divisao-de-licitacoes/

(3) http://ntic.unipampa.edu.br/compras

4.33.5. Análise da Auditoria:

O processo de planejamento das contratações de TIC na UNIPAMPA segue os seguintes passos:

1. Elaboração do Documento de Oficialização de Demanda pela Unidade requisitante.
2. Recebimento e análise do DOD, pelo NTIC.
3. Atendimento do requerimento por:

a. Estoque;
b. Carona Interna;
c. Emissão de pedido de compra.

Quanto a metas do processo, a única encontrada foi com relação ao prazo máximo para a apresentação do Documento de Oficialização de Demanda ao NTIC, formalizado em um calendário de oficialização de demandas de TIC e publicado em http://ntic.unipampa.edu.br/coordenacoes/coap/guia-de-compras. Não foram encontrados outros indicadores quantitativos e metas de processo a cumprir que possam ser considerados meios para mensuração do processo de planejamento. Sendo assim, a resposta ao item 5.8.c. não foi validada pela Auditoria, sendo considerada como prática adotada parcialmente.

4.34. Questão: **A organização executa processo de gestão de contratos de TI.** (Item: **5.9.b.**)

4.34.1. Resposta da Instituição: **Prática adotada: integral**

4.34.2. Contratos alisados: **10/2011 e 58/2014.**

4.34.3. Análise da Auditoria:

A responsabilidade de coordenar e comandar a gestão e fiscalização da execução contratual é do servidor designado como Gestor do contrato.

Como já observado, em ambos os contratos foi designado um Gestor, que adotou ações para melhor acompanhar a execução contratual, como mostrado no item seguinte. Sendo assim, a resposta ao item 5.9.b. foi validada pela Auditoria.

4.35. Questão: **O processo de gestão de contratos de TI é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.** (Item: **5.9.c.**)

4.35.1. Resposta da Instituição: **Prática adotada: parcial**

4.35.2. Contratos analisados: **10/2011 e 58/2014.**

4.35.3. Solicitação: comprovação de prática adotada integralmente (SA 061/2015).

4.35.4. **Resposta NTIC** (Memorando 074/2015)**:**

A fiscalização dos contratos atende a estrutura da IN 04/2014, em seu art. 2º, que cria os papéis de fiscal técnico, administrativo, requisitante e gestor atuando na fiscalização do serviço.

Esta fiscalização ocorre com base nos níveis de serviços acordados e dispostos no Termo de Referência da Contratação. Estes níveis de serviços definem um parâmetro mínimo de satisfação do serviço com base em prazos para retorno da contratada a partir de seu acionamento.

O acompanhamento de despesas das contratações também é uma importante ação conduzida pelo NTIC como forma de garantir a continuidade dos serviços. Com base na estimativa global do contrato, posteriormente informada no planejamento orçamentário do setor, os serviços contratados são monitorados de forma a estarem de acordo com os recursos financeiros disponíveis ao longo do período.

Esta análise motivou a implantação de uma política de uso para o contrato de impressões (PE 01/2011), que criou quotas de impressão para os usuários deste serviço (4). Também foi base de decisão para uma ação recente, referente ao fluxo de processo para abertura de chamados, do contrato de manutenção de redes (PE 35/2014), conforme Anexo 3.

O NTIC também adota pesquisas de satisfação para mensurar a aceitação do serviço aos usuários finais e fiscais locais, os resultados são utilizados como critério para renovação contratual (Anexo 4).[...]

(4) http://ntic.unipampa.edu.br/impressoes/quotas/

4.35.5. **Análise da Auditoria:**

De acordo com o Guia de Boas Práticas em Contratação de Soluções de TI (TCU), é na gestão contratual que o órgão efetivamente tem a possibilidade de obter os resultados pretendidos, compatíveis com os dispêndios previstos e com todo o esforço administrativo feito durante o processo licitatório. Também a IN 04, em seu artigo 31, afirma que a fase de Gestão do Contrato visa acompanhar e garantir a adequada prestação dos serviços e o fornecimento de bens que compõem a Solução de Tecnologia da Informação durante todo o período de execução do contrato.

De acordo com a resposta do Memorando, ambos os contratos passam por processos de acompanhamento dos serviços:

✓ Contrato nº 10/2011 (serviço de impressão): possui política de uso implantada, através da criação de quotas de impressão para os usuários do serviço.

✓ Contrato nº 58/2014 (manutenção de redes): passa por uma modificação referente ao fluxo de processo para abertura de novos chamados, na tentativa de redução de despesas, de forma a resguardar o uso do serviço até o final de sua vigência.

Próximo à data do encerramento do contrato, deve ser verificada a existência de interesse na renovação e encaminhada a documentação necessária para o aditivo. No caso de

assinatura de contrato com novo fornecedor, a providência tomada é a execução do processo de transição contratual. O contrato nº 58/2014 ainda não passou por nenhum desses processos, por ainda estar em vigência. Na primeira renovação do Contrato Nº 10/2011, observou-se a seguinte situação:

O Contrato originalmente tinha vigência de 12 meses a contar da assinatura (13/06/2011), podendo ser renovado até completar 60 meses. Porém, em 22 de agosto de 2012, o NTIC enviou Memorando ao Pró-Reitor de Administração da Universidade solicitando renovação imediata do contrato a contar de 12/06/2012, data anterior ao próprio memorando. O Contrato foi então aditivado, com data de 11/06/2012. O primeiro Termo Aditivo foi publicado no Diário Oficial da União em 25/09/2012.

De acordo com o parágrafo único da Lei 8.666/1993, a publicação resumida do instrumento de contrato ou aditamentos na imprensa oficial é condição indispensável para sua eficácia, devendo ser providenciada até o quinto dia útil do mês seguinte ao de sua assinatura, para ocorrer no prazo de vinte dias daquela data, qualquer que seja o valor, ainda que sem ônus, ressalvado o disposto no art. 26 da Lei. A inobservância desse dispositivo acarreta a responsabilidade dos agentes administrativos que descumpriram tal dever e adia o início do cômputo dos prazos contratuais.

Ainda com relação ao Contrato Nº 10/2011, observou-se que seu valor estimado era R$ 224.496,00. Porém, durante o período do segundo Termo Aditivo (13/06/2013 a 12/06/2014), o valor empenhado chegou a R$ 601.003,65, o que corresponde a um acréscimo de mais de 165%. Com relação a acréscimos e supressões contratuais, o Art. 65 da Lei 8.666/1993 apresenta:

> § 1º O contratado fica obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem nas obras, serviços ou compras, até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, e, no caso particular de reforma de edifício ou de equipamento, até o limite de 50% (cinquenta por cento) para os seus acréscimos.
>
> § 2º Nenhum acréscimo ou supressão poderá exceder os limites estabelecidos no parágrafo anterior, salvo:
>
> I - (VETADO)
>
> II - as supressões resultantes de acordo celebrado entre os contratantes.

De acordo com o Caderno de Logística: prestação de serviços de Reprografia[15], a utilização de software de gerenciamento é aplicável para contratações que envolvam um número significativo de máquinas concentradas em único local físico ou quando a quantidade de cópias contratadas seja superior, por exemplo, a 20.000 cópias/mês. O software de gerenciamento de impressão é recomendado para a redução do custo total de impressão, por permitir a diminuição do número de cópias e desperdício, por meio do controle sobre a fila de impressão e eventual determinação de cotas para usuários.

[15] Caderno de Logística: prestação de serviços de reprografia/Ministério do Planejamento, Orçamento e Gestão, Secretaria de Logística e Tecnologia da Informação. Brasília: MP, 2014.

As impressões na UNIPAMPA são gerenciadas pelo software PAPERCUT, acessível na rede interna a todos os usuários impressores. A Auditoria reconhece a política de quotas de impressão, implantada em março de 2014, como uma boa prática adotada pelo NTIC, visando à equalização do acesso aos serviços de impressão e o uso racional de papel e toner. Ressalta-se que, ao iniciar a execução contratual, é importante considerar isoladamente os acréscimos e supressões, definindo o valor que poderá ser acrescido e suprimido.

Sendo assim, considerando os dois contratos analisados, a Auditoria considera adequada a resposta ao item 5.9.c, de prática adotada parcialmente.

4.36. Questão: **A organização executa processo de gerenciamento do catálogo de serviços.** (Item: **5.1.a.**)

4.36.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.36.2. Análise da Auditoria:

Na ITIL v3[16], o Gerenciamento do Catálogo de Serviços busca assegurar que o catálogo de serviços seja produzido e mantido atualizado, contendo informações precisas sobre todos os serviços em operação, bem como aqueles que estão sendo preparados para entrar em operação. O objetivo do Gerenciamento de Catálogo de Serviços é fornecer uma única fonte consistente de informações sobre todos os serviços acordados e garantir que esses serviços estão amplamente disponíveis para aqueles que têm permissão para acessá-los.

Conforme análise, as informações sobre os serviços acordados estão disponíveis em um link, o qual contém uma minuta de documento, que é o Catálogo de Serviços de TI. Nesse documento online, as informações são atualizadas, conforme evolução do levantamento dos serviços ofertados pelo Núcleo. Após acesso ao documento, verificou-se que, por estar em fase de construção, não pode ser considerado ainda um local de informações consistentes sobre serviços acordados. Sendo assim, a Instituição continua na mesma situação de prática não adotada, embora tenha iniciado o plano para adotar.

4.37. Questão: **A organização executa processo de gerenciamento da continuidade dos serviços de TI.** (Item: **5.1.c.**)

4.37.1. Resposta da Instituição: **Prática adotada: integral**

4.37.2. Solicitação de comprovação: Plano de Continuidade de Serviços de TI, Plano de Contingência ou equivalente (SA 044/2015).

4.37.3. Resposta NTIC (Memorando 055/2015):

[16] ITIL® (Information Technology Infrastructure Library)

O processo de gerenciamento da continuidade dos serviços de TI é um conjunto de ações sob responsabilidade da Coordenadoria de Segurança da Informação do NTIC.

Um dos mais relevantes é o monitoramento automático dos links de Internet. Em caso de indisponibilidade do link principal o acesso passa ser oferecido pelos links de contingência, com redirecionamento automático dos serviços. Isso ocorre tanto na unidades nas quais estão os data centers como nas unidades que precisam dos links para acesso remoto aos data centers.

Data center estes que migraram de uma política centralizada, de único ponto de falha, para um modelo composto por data center principal e secundário, de contingência (1). Desta forma, há a replicação de serviços essenciais, com réplicas que operam sincronizados nos data centers atuais da Reitoria e Alegrete, que podem operar de forma independente em caso de indisponibilidade de uma das instâncias e que em breve receberão ampliação na infraestrutura em consonância com as normas e melhores práticas para implantação de salas seguras.

Além destes também podem ser destacados o serviço de cópias de segurança (backups) de forma automática, com o objetivo de garantir a continuidade dos serviços no caso da ocorrência de incidentes.

(1) http://ntic.unipampa.edu.br/files/2014/11/EstrategiaImplantacaoDatacentersLinksRNP_Novembro_2014.pdf

4.37.4. Análise da Auditoria:

De acordo com a ISO/IEC 20000-1, continuidade do serviço é a capacidade para gerenciar riscos e eventos que poderiam ter sério impacto em um ou mais serviços, a fim de entregar continuamente os serviços, nos níveis acordados.

O gerenciamento da continuidade dos serviços foca na elaboração de um plano de continuidade com estratégias de recuperação de serviço caso algum desastre aconteça, garantindo que a TI irá continuar a fornecer os serviços essenciais apesar das crises.

Com a resposta acima e com o "Plano de Ação para Mitigação de Incidentes", constante do PDTIC (páginas 145-147), a Instituição satisfaz o processo de gerenciamento da continuidade dos serviços de TI, validando a resposta ao item 5.1.c.

4.38. Questão: **A organização mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes, incluindo os níveis de serviço definidos.** (Item: **5.2.a.**)

4.38.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.38.2. Solicitação de comprovação: Informação de onde está publicado o catálogo atualizado dos serviços de TIC, ou justificativa, caso permaneça a situação de prática não adotada (SA 044/2015)

4.38.3. Resposta NTIC (Memorando 055/2015)**:**

Em janeiro do corrente ano foi iniciado a série de reuniões com os gestores do NTIC para elaboração do Catálogo de Serviços de TI. A minuta do documento está disponível no endereço http://goo.gl/JNM5At, onde são atualizadas as informações, conforme evolução do levantamento dos serviços ofertados pelo núcleo.

Cabe esclarecer que esta tarefa demanda um tempo maior em sua fase inicial de elaboração pois o levantamento dos serviços exige uma definição clara quanto às responsabilidades, prazos (*SLA - service level agreement*) e trâmites necessários, o que impõe uma análise minuciosa dos processos internos.

Atualmente, as coordenadorias trabalham justamente na elaboração destas definições, para que seja finalizado o Catálogo para publicação no segundo semestre de 2015.

4.38.4. Análise da Auditoria:

O Catálogo de Serviços contém todos os serviços de TI que são oferecidos aos clientes e serviços que já foram liberados e que de fato vão entrar em operação. O Catálogo contém detalhes dos serviços, quais unidades de negócio os utilizam e os processos baseados nos serviços. O catálogo de serviço é um documento à parte que é visível para os clientes.

De acordo com a resposta acima, o Catálogo de Serviços de TI ainda está sendo elaborado. Por esse motivo, a prática continua não sendo adotada.

4.39. Questão: **A organização identifica os riscos de TI dos processos críticos de negócio.** (Item: **5.3.a.**)

4.39.1. Resposta da Instituição: **Prática adotada: integral**

4.39.2. Análise da Auditoria:

De acordo com o PDTIC, a UNIPAMPA utiliza os seguintes critérios para definir o nível de risco e a priorização do plano de ações:

- Número de usuários impactados;
- Impacto das demandas e exigências legais dos ministérios;
- Exigências normativas e legais dos órgãos controladores;
- Alinhamento estratégico com a Instituição;
- Custo financeiro de executar ou não o projeto;
- Quantidade de sistemas impactados;
- Impacto na imagem da Instituição junto à comunidade;
- Impacto na imagem do NTIC junto à Instituição;
- Tempo para conclusão do projeto;
- Quantidade de pessoas envolvidas;
- Qualificação necessária dos recursos humanos envolvidos;
- Outros, adequados à boa priorização e encaminhamento dos projetos.

Além disso, também há no PDTIC o Mapa de Risco por Projeto, onde são identificados os principais riscos associados a não execução de cada projeto do Portfólio. Como os projetos são para atender às áreas de negócio da Instituição, se pode afirmar que a organização identifica os riscos de TI dos processos críticos de negócio. Sendo assim, a Auditoria validou a resposta ao item 5.3.a.

4.40. Questão: **A organização executa um processo de software, com o objetivo de assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades.** (Item: **5.5.a.**)

4.40.1. Resposta da Instituição: **Prática adotada: integral**

4.40.2. Solicitação de comprovação: Tabela contendo softwares desenvolvidos e em desenvolvimento, com a informação do modelo de referência utilizado para cada um deles e a área da Instituição que foi atendida (SA 044/2015).

4.40.3. **Resposta NTIC** (Memorando 055/2015):

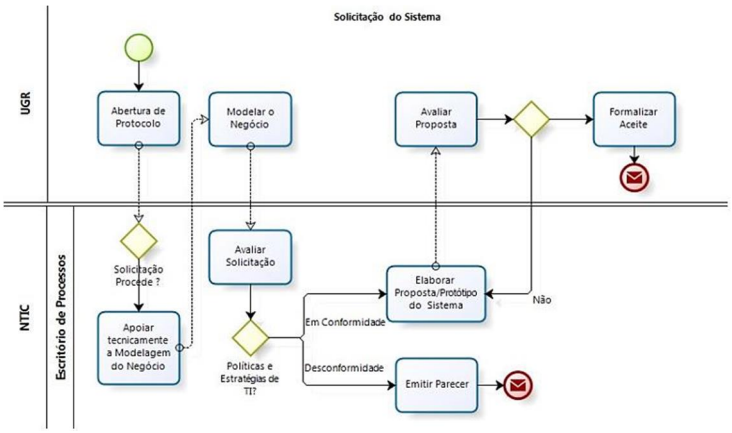
A Coordenadoria de Apoio ao Usuário é responsável pelo recebimento e análise de demandas de desenvolvimento de softwares, iniciando uma série de etapas com o objetivo de conceber um projeto para posterior desenvolvimento. A etapa principal consiste especificamente no levantamento de requisitos, momento em que serão especificadas todas as funções que deverão envolver a ferramenta, com alto nível de detalhamento. Em conjunto com a Coordenadoria de Desenvolvimento são realizadas reuniões para testes e verificação destes requisitos. Este processo de interação foi modelado e está publicada no site do NTIC (1).

(1) http://ntic.unipampa.edu.br/coordenacoes/codev10/processos-internos/

4.40.4. **Análise da Auditoria:**

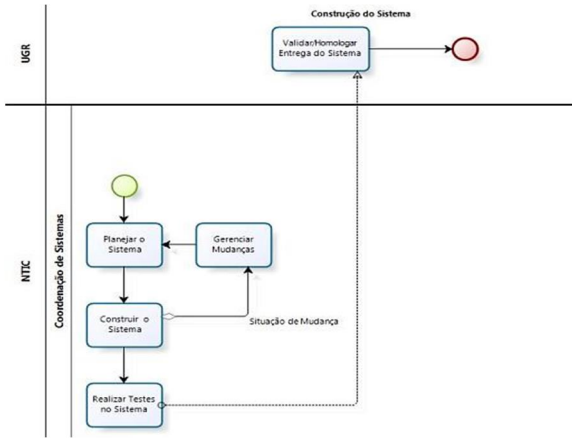
De acordo com o Processo de Software para o SISP – PSW - SISP, o processo de software é composto pelas fases Concepção e Alinhamento Estratégico, Especificação e Dimensionamento, Estratégia de Desenvolvimento, Desenvolvimento, Implantação e Estabilização, Sustentação e Evolução. No Anexo VII do PDTIC da UNIPAMPA – Proposta de Projeto de Desenvolvimento de Software - consta um modelo de processo de registro e encaminhamento de demandas:

Figura 4 – 1ª etapa: Solicitação do desenvolvimento



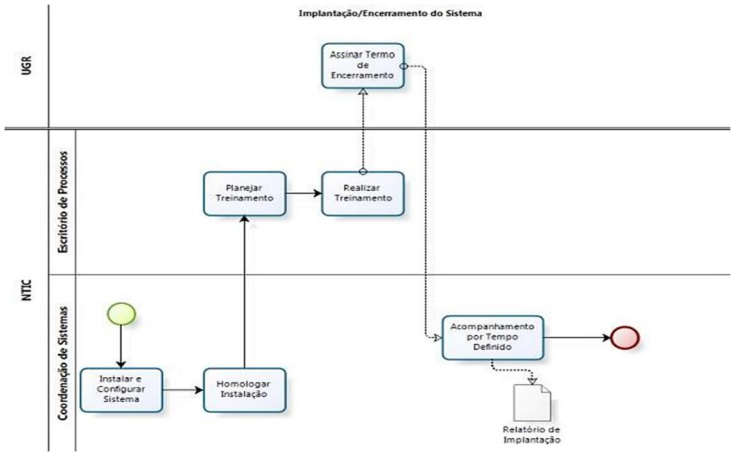
FONTE: PDTIC UNIPAMPA

Figura 5 – 2ª etapa: Construção do Sistema



FONTE: PDTIC UNIPAMPA

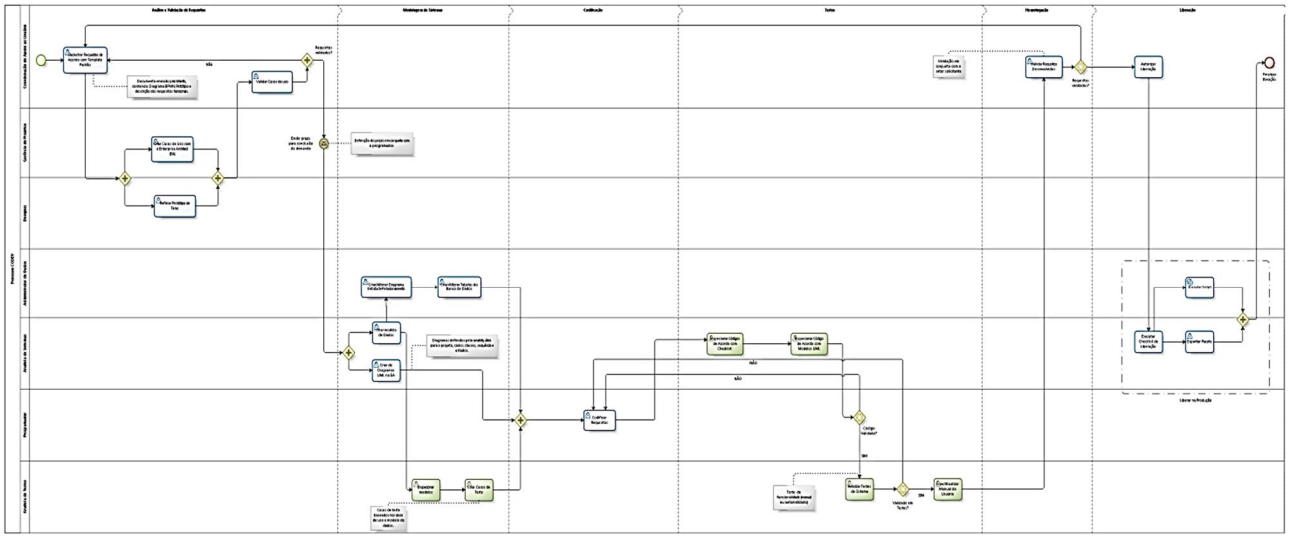
Figura 6 - 3ª etapa: Implantação e Encerramento do Sistema



FONTE: PDTIC UNIPAMPA

Pode-se observar que o processo adotado pelo NTIC representa um modelo simplificado do modelo do SISP. Porém, não foram apresentadas à Auditoria tabelas contendo softwares desenvolvidos e em desenvolvimento, com a informação do modelo de referência utilizado para cada um deles e a área da Instituição que foi atendida, como solicitado na SA nº 044/2015.

Após apresentação deste Relatório Preliminar, o Gestor apresentou o processo de software atualmente executado na Instituição, revisado em outubro de 2015:



Também foram apresentados documentos comprobatórios do efetivo funcionamento do processo de software. Sendo assim, a resposta ao item 5.5.a. foi validada pela Auditoria.

4.41. Questão: **A organização possui portfólio de projetos de TI.** (Item: **5.6.a.**)

4.41.1. Resposta da Instituição: **Prática não adotada: iniciou plano**

4.41.2. Análise da Auditoria:

O Portfólio de Projetos de TI está no PDTIC, nas páginas 61 a 110. Os projetos estão divididos em transversais, infraestrutura e desenvolvimento. "Os projetos transversais são projetos administrativos, de gestão e/ou projetos que envolvem tanto a área de infraestrutura quanto a área de desenvolvimento. Os projetos de infraestrutura são aqueles classificados como básica e puramente de implantação e/ou consolidação das bases tecnológicas necessárias ao funcionamento da instituição e ao desenvolvimento de outros projetos, como os de desenvolvimento. Por fim, os projetos de desenvolvimento englobam basicamente sistemas e soluções de software cujo objetivo é prestar serviços necessários à instituição e a comunidade". (PDTIC, página 62)

Sendo assim, a Instituição saiu da situação de prática não adotada para a de prática adotada integralmente.

4.42. Questão: **A organização executa processo de gerenciamento de projetos de TI.** (Item: **5.6.b.**)

4.42.1. Resposta da Instituição: **Prática adotada: parcial**

4.42.2. Solicitação de comprovação: Tabela contendo projetos executados e em execução, com a informação do coordenador de cada um, acompanhamento de suas fases e o critério utilizado para priorização (SA 044/2015).

4.42.3. Resposta NTIC (Memorando 055/2015)**:**

Este gerenciamento é responsabilidade conjunta da Coordenadoria de Apoio ao Usuário (CAU) e da Coordenadoria de Desenvolvimento de Sistemas (CODEV), com base nos requisitos e informações do projeto que podem influenciar sua priorização na fase de desenvolvimento ou execução.

As informações sobre projetos desenvolvidos ou em desenvolvimento podem ser visualizadas por meio do sistema adotado no NTIC para esta finalidade, disponível no site do NTIC (1).

(1) http://testes.unipampa.edu.br/mantis/estatisticas/

4.42.4. Análise da Auditoria:

De acordo com a Metodologia de Gerenciamento de Portfólio de Projetos do SISP, gerenciamento de projetos é a aplicação de conhecimentos, habilidades e técnicas às atividades de um projeto, a fim de atingir seus objetivos.

Através do link apontado pelo NTIC, foi possível pesquisar os projetos que estão em desenvolvimento, finalizados e a serem desenvolvidos, bem como as informações solicitadas na SA 044/2015, exceto os critérios de priorização. O NTIC também utiliza softwares para auxiliar no gerenciamento de projetos, como o Redmine, que é um software gerenciador de projetos, e o Mantis Bug Tracker, uma ferramenta de gestão de falhas em outros softwares.

Considerando o exposto acima, a Auditoria considerou que os projetos de TIC estão sendo integralmente gerenciados na Instituição.

4.43. Questão: **A organização possui um escritório de projetos, ao menos para projetos de TI.** (Item: **5.6.f.**)

4.43.1. Resposta da Instituição: **Prática adotada: integral**

4.43.2. Solicitação de comprovação: Estrutura de funcionamento, principais atribuições e equipe responsável pelo escritório de projetos (SA 044/2015).

4.43.3. Resposta NTIC (Memorando 055/2015)**:**

Dentre os objetivos que fomentaram a criação da Coordenadoria de Apoio ao Usuário (CAU) estão os que foram atribuídos como responsabilidade do "Escritório de processos de TI": (i) Apoiar os gestores (Alta administração da UNIPAMPA) no acompanhamento e avaliação das demandas de TI; (ii) Avaliar o portfólio de recursos de TI da instituição e contribuir na sua administração; (iii) Integrar os múltiplos processos e gestores de processos consolidando suas demandas de TI; (iv) Consolidar os registros e documentações de diferentes gestores, avaliar as melhores práticas e definir as melhores formas de atendimento das demandas; (v) Ser interlocutor entre os diversos setores da Universidade e o NTIC; (vi) Garantir o alinhamento das demandas de TI ao planejamento estratégico da organização; (vii) Treinar e capacitar o pessoal com os recursos de TI, disponibilizados e devidamente documentados pelo NTIC; e (viii) Identificar a existência de processos repetitivos, que possam ser otimizados através de recursos de TI, e propor sua automatização a fim de reduzir os custos.

Estas atividades incluem o mapeamento e a modelagem dos processos junto aos diferentes setores da instituição, sendo os responsáveis pelo recebimento e análise de demandas e definição do escopo dos projetos de TI, envolve, inclusive, a mobilização das demais coordenadorias do NTIC no apoio técnico e alinhamentos quanto a priorização da alocação de recursos para execução. A equipe é composta por quatro Analistas de Tecnologia da Informação, possuindo capacitação na aplicação da metodologia BPM.

(1) http://ntic.unipampa.edu.br/coordenacoes/cau/

4.43.4. Análise da Auditoria:

De acordo com o PMBOK, 5ª edição, um escritório de gerenciamento de projetos é uma estrutura organizacional que padroniza os processos de governança relacionados a projetos e facilita o compartilhamento de recursos, metodologias, ferramentas, e técnicas.

A partir do exposto no memorando, a Auditoria validou a resposta ao item 5.6.f.

5. CONSTATAÇÕES

5.1. Constatação 1

A organização prioriza parcialmente as ações de TI com apoio do comitê de TI (ou colegiado equivalente), que atua como instância consultiva da alta administração.

5.1.1. Critérios

- ✓ Guia de Comitê de TI do SISP: versão 2.0/Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação - Brasília: MP, 2013.
- ✓ Nota Técnica 7/2014 - Sefti/TCU – versão 2.8.

5.1.2. Evidências

- ✓ Memorando NTIC 035/2015 – Resposta à SA 022/2015.
- ✓ Atas das reuniões do CGTIC.

5.1.3. Análise do gestor sobre a constatação

"Considerando a objetividade da questão, permitindo entender que, quando há necessidade de priorizar ações de TI, o CGTIC é envolvido como apoiador da causa, que naturalmente envolvem discussões que antecedem uma possível normativa ou política institucional. Portanto, reafirmamos que a organização prioriza as ações de TI com apoio do comitê de TI, inclusive quando esta necessidade é apontada pela alta administração, consequentemente, como parte deste processo, também atuando como instância consultiva."

5.1.4. Conclusão da Auditoria

A Auditoria entende que, para a prática ser considerada como adotada na Instituição, o Comitê de TI deve ser um dos envolvidos na priorização das ações de TI. Dessa forma, para que uma ação de TI seja considerada como prioridade, deverá anteriormente ter passado por apreciação e aprovação em reunião do CGTIC, que atuará como instância consultiva da alta administração na decisão de priorizar ou não ações de TI. Essa atuação não foi observada pela Auditoria nas respostas às Solicitações de Auditoria, nem nas atas das reuniões do CGTIC. A recomendação foi reformulada para melhor entendimento do que foi explicitado acima.

5.1.5. Recomendação

1. Recomenda-se que, para a priorização de ações de TI, haja apreciação e aprovação da matéria pelo CGTIC.

5.2. Constatação 2

A organização define parcialmente diretrizes para gestão do portfólio de projetos e serviços de TI, inclusive para definição de critérios de priorização e de alocação orçamentária.

5.2.1. Critérios

✓ Nota Técnica 7/2014 - Sefti/TCU – versão 2.8.

✓ Metodologia de Gerenciamento de Portfólio de Projetos do SISP/Ministério do Planejamento, Orçamento e Gestão. Secretaria de Logística e Tecnologia da Informação – 2013.

5.2.2. Evidências

✓ Memorando NTIC 035/2015 – Resposta à SA 022/2015.

✓ Memorando NTIC 061/2015 e anexos - Resposta à SA 049/2015.

5.2.3. Análise do gestor sobre a constatação

"A questão (Item: 1.3.b.) trata da formalização de diretrizes para gestão de portfólio de projetos e serviços de TI, o que entendemos que faça referência principalmente ao método utilizado para tal definição e formalização, o que já foi demonstrado por meio da publicação do PDTIC da universidade. Entretanto, reconhecemos que tais diretrizes estão desatualizadas e que precisam ser revisadas e publicadas, em consonância com as recomendações desta Constatação."

5.2.4. Conclusão da auditoria

A Auditoria mantem as duas recomendações, visto que as diretrizes para priorização estão desatualizadas e que a informação do critério utilizado para a priorização de cada projeto trará maior transparência ao processo.

5.2.5. Recomendações

2. Recomenda-se que sejam publicadas as alterações de diretrizes para gestão do portfólio de projetos e serviços de TIC, em razão das decisões tomadas nas reuniões periódicas com a alta gestão, preferencialmente em versão revisada anual do PDTIC.

3. Recomenda-se que os projetos priorizados sejam acompanhados da informação do critério utilizado para sua priorização.

5.3. Constatação 3

A organização define parcialmente diretrizes para avaliação do desempenho dos serviços de TIC.

5.3.1. Critérios

✓ ABNT NBR ISO/IEC 20000

5.3.2. Evidências

✓ Memorando NTIC 035/2015 – Resposta à SA 022/2015.

✓ PDTIC UNIPAMPA - fevereiro 2011.

✓ PDI UNIPAMPA 2014-2018.

5.3.3. Análise do gestor sobre a constatação

"Assim como no item anterior, entendemos que a organização define formalmente as diretrizes para avaliação do desempenho dos serviços, porém neste momento as mesmas estão desatualizadas, devendo ser revisadas e publicadas."

5.3.4. Conclusão da auditoria

As considerações da Auditoria sobre essa questão sofreram algumas alterações, no item 4.6.4 deste Relatório, porém manteve-se a recomendação, que vai ao encontro da manifestação do Gestor sobre a desatualização de diretrizes para avaliação de desempenho.

Recomendação

4. Recomenda-se revisão de metas e indicadores, bem como sua publicação em versão revisada anual do PDTIC.

5.4. Constatação 4

O PDTI vigente contempla objetivos, indicadores e metas para a TIC, porém os objetivos não são explicitamente alinhados aos objetivos de negócio constantes do PDI.

5.4.1. Critérios

✓ Guia de PDTI do SISP – Versão 2.0 beta – Brasília, 2015.

5.4.2. Evidências

✓ Memorando NTIC 043/2015 – Resposta à SA 031/2015.

✓ PDTIC UNIPAMPA - fevereiro 2011.

✓ PDI UNIPAMPA 2014-2018.

5.4.3. Análise do gestor sobre a constatação

"O alinhamento entre as ações estratégicas de TI e os objetivos institucionais devem ser atualizados na revisão do PDTIC. Há de se salientar, porém, que o PDTIC vigente foi desenvolvido tomando por base o primeiro PDI da universidade, com vigência até 2013."

5.4.4. Conclusão da auditoria

As considerações da Auditoria sobre essa questão sofreram algumas alterações, no item 4.13.4 deste Relatório, porém manteve-se a recomendação.

5.4.5. Recomendações

5. Recomenda-se que, para os próximos planejamentos de TIC, seja explicitado o alinhamento dos objetivos do Plano de TIC com os objetivos de negócio que constam do Planejamento Estratégico Institucional, demonstrando assim como as necessidades de TIC apresentadas se relacionam com os objetivos institucionais.

5.5. Constatação 5

A organização não dispõe de uma política de segurança da informação formalmente instituída, como norma de cumprimento obrigatório.

5.5.1. Critérios

✓ Guia de Orientações ao Gestor em Segurança da Informação e Comunicações – DSIC/GSIPR.

✓ Norma Complementar Nº 03/IN01/DSIC/GSIPR.

5.5.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.5.3. Análise do gestor sobre a constatação

"O NTIC aguarda a formalização da Estrutura de Segurança da Informação e Comunicação da UNIPAMPA - ESIC, que será composto, entre outros, pelo Comitê de Segurança da Informação e Comunicações (CSIC), grupo responsável pela criação da política de segurança da informação da universidade."

5.5.4. Conclusão da auditoria

A Auditoria entende que, por já existir a Resolução nº 83/2014, a qual institui a Estrutura de Segurança da Informação e Comunicações (ESIC), faltando apenas publicação da nova estrutura organizacional da Universidade contendo a ESIC, não há recomendações a serem feitas.

5.5.5. Recomendação

-

5.6. <u>Constatação 6</u>

A organização não dispõe de Comitê de Segurança da Informação formalmente instituído.

5.6.1. Critérios

✓ Guia de Orientações ao Gestor em Segurança da Informação e Comunicações – DSIC/GSIPR.

✓ Norma Complementar Nº 03/IN01/DSIC/GSIPR.

5.6.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.6.3. Análise do gestor sobre a constatação

"Houveram avanços recentes para criação da Estrutura de Segurança da Informação e Comunicação da UNIPAMPA - ESIC, que será composto, entre outros, pelo Comitê de Segurança da Informação e Comunicações (CSIC). A minuta da resolução de criação foi enviada para o CONSUNI e aguarda deliberação daquele conselho para formalização do grupo."

5.6.4. Conclusão da auditoria

A Auditoria entende que, por já existir a Resolução nº 83/2014, a qual institui a Estrutura de Segurança da Informação e Comunicações (ESIC), faltando apenas publicação da nova estrutura organizacional da Universidade contendo a ESIC, não há recomendações a serem feitas.

5.6.5. Recomendação

-

5.7. <u>Constatação 7</u>

A organização não dispõe de política de cópias de segurança (backup) formalmente instituída.

5.7.1. Critérios

✓ Boas Práticas em Segurança da Informação – TCU.

5.7.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.7.3. **Análise do gestor sobre a constatação**

"A UNIPAMPA possui política formal de cópias de segurança já que existe processo de backup periódico de todos os sistemas administrados pelo NTIC, inclusive com planos de teste de integridade, sob responsabilidade formal da Coordenadoria de Segurança de Informação (CSI). Contundo, entende-se que esta política deve ser ampliada, o que deverá estar contemplado na POSIC, cuja criação será atribuição do Comitê de Segurança da Informação e Comunicações (CSIC) após sua formalização."

5.7.4. Conclusão da auditoria

Conclui-se que é necessária apenas a publicação da nova estrutura organizacional da Universidade contendo a ESIC, o que permitirá a existência de uma política de segurança da informação formalmente instituída, a qual contemplará, entre outros, a política formal de cópias de segurança (backups). Com base na manifestação do gestor, a Auditoria reconhece a existência de processo de backup periódico de todos os sistemas administrados pelo NTIC, não havendo recomendações a serem feitas.

5.7.5. Recomendação

-

5.8. <u>Constatação 8</u>

A organização executa parcialmente processo de gestão de riscos de segurança da informação.

5.8.1. Critérios

✓ Norma Complementar Nº 04/IN01/DSIC/GSI/PR.

✓ ABNT NBR ISO 31000: 2009 - Gestão de riscos — Princípios e diretrizes.

5.8.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.8.3. Análise do gestor sobre a constatação

"Discordamos que atualmente a gestão de riscos seja executado parcialmente, visto que o NTIC possui em sua estrutura uma Coordenadoria com atribuição legítima para esta gestão, executando diversas ações neste sentido, conforme exposto no Memorando 055/2015-NTIC. Os métodos e padrões, entretanto, precisam ser formalizados, o que deve ocorrer após a criação da Estrutura de Segurança da Informação e Comunicação da UNIPAMPA - ESIC."

5.8.4. Conclusão da auditoria

A Auditoria reformulou as considerações sobre a questão no item 4.23.4 deste Relatório, eliminando a recomendação e validando a questão 5.4.k.

5.8.5. Recomendação

-

5.9. Constatação 9

A organização não possui equipe de tratamento e resposta a incidentes de segurança em redes computacionais formalmente instituída.

5.9.1. Critérios

✓ Norma Complementar Nº 05/IN01/DSIC/GSIPR e Anexo A.

✓ Guia de Orientações ao Gestor em Segurança da Informação e Comunicações – DSIC/GSIPR.

5.9.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.9.3. Análise do gestor sobre a constatação

"Reiteramos o que foi informado no Memorando 055/2015-NTIC: a organização possui uma equipe de tratamento e resposta a incidentes de segurança (ETIR), que, embora não esteja inserido na ESIC, é formalmente constituída na Coordenadoria de Segurança da Informação, parte integrante da estrutura do NTIC, com atribuição legítima para serviços na área de segurança da informação. Ou seja, com a criação da ESIC, esta atribuição e parte da equipe da CSI migrará para a ETIR da ESIC."

5.9.4. Conclusão da auditoria

Após verificação da manifestação do gestor, a Auditoria concluiu que a Instituição possui Equipe de Tratamento e Resposta a Incidentes de Segurança (ETIR). As considerações sobre a questão foram reformuladas no item 4.25.4 deste Relatório.

Sendo assim, a recomendação foi retirada, e a resposta à questão 5.4.s. validada.

5.9.5. Recomendação

-

5.10. Constatação 10

A estrutura de SIC da Instituição não está plenamente constituída.

5.10.1. Critérios

✓ Resolução UNIPAMPA nº 83/2014.

5.10.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.10.3. Análise do gestor sobre a constatação

"Conforme mencionado na Constatação 6, o NTIC aguarda deliberação do CONSUNI sobre as alterações na estrutura da universidade contemplando a ESIC."

5.10.4. Conclusão da auditoria

A Auditoria entende que, por já existir a Resolução nº 83/2014, a qual institui a Estrutura de Segurança da Informação e Comunicações (ESIC), faltando apenas publicação da nova estrutura organizacional da Universidade contendo a ESIC, não há recomendações a serem feitas.

5.10.5. Recomendação

-

5.11. Constatação 11

A organização não explicita, nos autos do processo de contratação, os indicadores dos benefícios de negócio que serão alcançados.

5.11.1. Critérios

✓ Guia de boas práticas em contratação de Soluções de Tecnologia da Informação - MPOG - SLTI.

✓ Instrução Normativa N° 4 - SLTI, de 11 de Setembro de 2014.

5.11.2. Evidências

✓ Contratos 10/2011 e 58/2014.

5.11.3. Análise do gestor sobre a constatação

"Acatamos a constatação e recomendação sem nada mais a acrescentar."

5.11.4. Conclusão da auditoria

Com base na manifestação, conclui-se que serão tomadas providências para que os benefícios de negócio a serem alcançados sejam acompanhados por indicadores nos autos do processo de contratação.

5.11.5. Recomendação

6. Recomenda-se que os benefícios de negócio a serem alcançados estejam acompanhados por indicadores nos autos do processo de contratação.

5.12. Constatação 12

A organização não adota métricas objetivas para mensuração de resultados do contrato.

5.12.1. Critérios

✓ Guia de boas práticas em contratação de Soluções de Tecnologia da Informação - MPOG - SLTI.

✓ Instrução Normativa N° 4 - SLTI, de 11 de Setembro de 2014.

5.12.2. Evidências

✓ Contratos 10/2011 e 58/2014.

5.12.3. Análise do gestor sobre a constatação

"Acatamos a constatação e recomendação sem nada mais a acrescentar."

5.12.4. Conclusão da auditoria

Com base na manifestação, conclui-se que serão tomadas providências para adoção de métricas objetivas para mensuração de resultados dos contratos.

5.12.5. Recomendação

7. Recomenda-se que sejam adotadas métricas objetivas para mensuração de resultados dos contratos.

5.13. Constatação 13

O processo de planejamento das contratações de TI não é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

5.13.1. Critérios

✓ Guia de boas práticas em contratação de Soluções de Tecnologia da Informação - MPOG - SLTI.

✓ Instrução Normativa N° 4 - SLTI, de 11 de Setembro de 2014.

5.13.2. Evidências

✓ Contratos 10/2011 e 58/2014.

5.13.3. Análise do gestor sobre a constatação

"Acatamos a constatação e recomendação sem nada mais a acrescentar."

5.13.4. Conclusão da auditoria

Com base na manifestação, conclui-se que serão tomadas providências para que haja o acompanhamento do processo de planejamento das contratações de TIC.

5.13.5. Recomendação

8. Recomenda-se que haja acompanhamento do processo de planejamento das contratações de TIC, através da utilização de indicadores e metas de processo a cumprir.

5.14. Constatação 14

O processo de gestão de contratos de TI não é acompanhado por meio de mensurações, com indicadores quantitativos e metas de processo a cumprir.

5.14.1. Critérios

✓ Guia de boas práticas em contratação de Soluções de Tecnologia da Informação - MPOG - SLTI.

✓ Instrução Normativa N° 4 - SLTI, de 11 de Setembro de 2014.

5.14.2. Evidências

✓ Contratos 10/2011 e 58/2014.

5.14.3. Análise do gestor sobre a constatação

"Acatamos a constatação e recomendação sem nada mais a acrescentar."

5.14.4. Conclusão da auditoria

Com base na manifestação, conclui-se que serão tomadas providências para maior rigor no processo de gestão dos contratos de TIC.

5.14.5. Recomendação

9. Recomenda-se que o processo de gestão dos contratos de TIC seja mais rigoroso, principalmente no que diz respeito a aspectos legais sobre prazos de renovação e acréscimos em valores contratados.

5.15. Constatação 15 e Constatação 16

A organização não executa processo de gerenciamento do catálogo de serviços.

A organização não mantém um catálogo publicado e atualizado dos serviços de TI oferecidos às áreas clientes.

5.15.1. Critérios

✓ ABNT NBR ISO/IEC 20000.

5.15.2. Evidências

✓ Memorando NTIC 043/2015 - Resposta à SA 031/2015.

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.15.3. Análise do gestor sobre a constatação

"Acatamos a constatação e recomendação sem nada mais a acrescentar."

5.15.4. Conclusão da auditoria

Com base na manifestação, conclui-se que serão tomadas providências para a finalização do Catálogo de Serviços de TIC, bem como disponibilização às áreas clientes para acessá-lo.

5.15.5. Recomendação

10. Recomenda-se a finalização do Catálogo de Serviços de TIC, bem como disponibilização às áreas clientes para acessá-lo.

5.16. <u>Constatação 17</u>

A organização não executa um processo de software, com o objetivo de assegurar que o software a ser desenvolvido, direta ou indiretamente, atenda às suas necessidades.

5.16.1. Critérios

✓ Processo de Software para o SISP – PSW - SISP.

✓ Anexo VII do PDTIC da UNIPAMPA.

5.16.2. Evidências

✓ Memorando NTIC 055/2015 - Resposta à SA 044/2015.

5.16.3. Análise do gestor sobre a constatação

"Discordamos desta constatação pois o processo de desenvolvimento de software na instituição foi formalmente instituído por meio do PDTIC e posteriormente refinado em função da criação da CAU e redefinição das atribuições da CODEV. Em anexo são apresentados artefatos que comprovam a instituição e o efetivo funcionamento do processo."

5.16.4. Conclusão da auditoria

A Auditoria analisou os novos documentos enviados e concorda com a manifestação do gestor de que há processo de software em execução na Instituição, atualizando as considerações no item 4.40.4 deste Relatório. Sendo assim, a recomendação foi eliminada e a resposta ao item 5.5.a. foi validada pela Auditoria.

5.16.5. Recomendação

-

6. RESPOSTAS ÀS QUESTÕES DE AUDITORIA

Na fase de planejamento da Auditoria, foram formuladas questões de Auditoria, partindo-se do objetivo e do escopo deste trabalho. A partir da execução dos trabalhos de Auditoria, foi possível chegar às seguintes respostas:

6.1. Existe política de Governança em TIC implementada na Instituição?

Levando-se em consideração as respostas validadas, as não validadas e as questões que permanecem em situação de não atendidas ou atendidas parcialmente, concluiu-se que a política de Governança em TI está em implementação na Instituição. O principal ponto a ser corrigido, de acordo com avaliação desta Auditoria, diz respeito à definição e ao esclarecimento dos critérios utilizados na priorização das ações de TIC.

Para alcançar os objetivos estratégicos da Instituição, faz-se necessário realizar projetos de TIC, porém a escassez de recursos torna imperativo escolher quais projetos. Para essa escolha, precisa-se minimamente: (i) definir a estratégia, objetivos e metas da organização; (ii) desdobrar esses objetivos e metas em critérios de seleção e priorização que permitam comparar as propostas de projetos de maneira objetiva e imparcial. O item (i) já foi feito pela UNIPAMPA, e está materializado nos Planejamentos Estratégicos do PDI e PDTIC. Posteriormente, a Instituição precisa definir objetivamente quais são as diretrizes para gestão do portfólio de projetos e serviços de TIC, inclusive para definição de critérios de priorização e de alocação orçamentária. Ressalta-se que o Gerenciamento de Portfólio é um dos Processos de Governança Corporativa de TI (APO05) do COBIT® 5 [17].

De acordo com a Nota Técnica nº 07/2014 – TCU, para que os dirigentes tenham condições de governar a TI, convém que seja adotado o ciclo “avaliar-dirigir-monitorar”, pelo qual primeiro se realiza a avaliação do uso atual e futuro da TI com base nas necessidades do negócio. Em seguida deve ser definida a direção da TI na organização, mediante princípios e diretrizes que estabeleçam a forma de atuação da gestão da TI, bem como planos que definam a direção dos investimentos nos projetos e operações de TI. Por fim, a alta administração monitora o desempenho obtido pela TI em função da direção previamente estabelecida, valendo-se de processos e sistemas de mensuração apropriados. O fato de a organização definir parcialmente diretrizes para avaliação do desempenho dos serviços de TI revela uma falha no sistema de monitoramento e, consequentemente, na Governança de TI.

Com relação aos sistemas informatizados que dão suporte aos principais processos de negócio da Instituição, a Auditoria sugere que todos os usuários do sistema GURI possam visualizar todos os módulos existentes, embora tenham acesso somente aos que forem pertinentes ao desenvolvimento do seu trabalho. Dessa maneira, possibilita-se maior ciência quanto às funcionalidades e recursos existentes para desenvolvimento de processos na Instituição.

[17] COBIT® 5 - Modelo Corporativo para Governança e Gestão de TI da Organização

6.2. As metas propostas no PDTIC e no PDI estão sendo alcançadas e alinhadas entre si?

Após análise das comprovações enviadas à Auditoria e dos documentos e informações pertinentes, concluiu-se que as metas do PDTIC estão sendo alcançadas e que há monitoramento quanto a sua execução.

Quanto ao alinhamento entre os Planos, pode-se afirmar que foi observada a Missão da Instituição para compor o Mapa Estratégico do NTIC e a definição de seus objetivos, indicadores e metas, mas que não há alinhamento explícito entre os objetivos de negócio da Instituição e os objetivos, indicadores e metas do PDTIC.

6.3. São executadas ações que permitam a existência de estrutura de Segurança da Informação e Comunicações na Instituição?

São executadas diversas ações de segurança da informação e comunicações na Instituição, porém, por falta de formalização, essas ações não são capazes de constituir uma estrutura sólida de SIC. A falta de formalização da composição da ESIC e seus componentes básicos, como a POSIC, CSIC, GSIC, ETIR, entre outros, torna as ações de SIC frágeis, isoladas e, consequentemente, não institucionalizadas. Por esse motivo, é possível concluir que a estrutura de SIC da Instituição não está plenamente constituída.

Nesse ponto, faz-se necessário o breve relato do incidente de segurança da informação de perda de dados ocorrido em 19/10/2013, que teve como causa principal uma queda de energia no datacenter em Alegrete, concomitantemente à falha nas ferramentas de alta disponibilidade adotadas pelo Núcleo. O Relato completo está no Anexo recebido em resposta à SA nº 060/2015.

O incidente foi agravado pelo fato de que o Bacula – ferramenta utilizada para gerar backups – também estava operando em uma máquina virtual que foi corrompida no evento. No caso de ocorrer um problema de perda de dados no local primário de armazenamento ou de indisponibilidade da aplicação, o Bacula permite recuperar os dados dos usuários da aplicação, bem como os dados de configuração da própria aplicação, permitindo que o serviço seja restabelecido com as condições do último backup realizado. Porém, a equipe da CSI havia optado por usar o Dell PowerVault – equipamento primário de armazenamento de dados do NTIC (storage) – como dispositivo de armazenamento de dados do Bacula. O motivo dessa decisão foi a concepção de que o PowerVault apresenta tolerância a falhas, associada à falta de um segundo equipamento para armazenamento de cópias de segurança (backup).

Sobre as medidas tomadas para prevenção de novos incidentes de segurança, a direção do NTIC tem trabalhado junto com os responsáveis pelas Coordenadorias para qualificar os processos, possibilitar atingir níveis satisfatórios de disponibilidade e, principalmente, evitar ao máximo a possibilidade de perda de dados institucionais. A importância do armazenamento de dados tem sido foco das ações das Coordenadorias, sendo que equipamentos foram deslocados de outras demandas para a criação de servidores de armazenamento e para disponibilizar máquinas virtuais com capacidade suficiente para que os serviços apresentem desempenho aceitável para a execução das tarefas acadêmico-administrativas.

6.4. O processo de aquisição de bens e serviços de TIC é realizado de maneira a agregar valor aos objetivos Institucionais?

A aquisição de bens e serviços de TIC não pode ser vista de maneira isolada, visto que deve estar inserida em um contexto de auxílio no alcance dos objetivos Institucionais. A TIC não deve ter processos com fim em si mesmos, pois assim dificilmente contribuirá com a Instituição na qual está inserida, tornando-se um setor à parte e com aquisições que não agregam valor ao resto da Instituição.

Após análise dos itens, verificou-se que, apesar de alguns não terem sido validados pela Auditoria e terem a recomendação de melhoria, o setor de Compras do NTIC vem tomando medidas para que o processo de contratações atenda da melhor maneira possível os requisitos legais e de alinhamento com os objetivos da Instituição. Porém, é preciso que se avalie melhor a gestão de contratos, para que se evitem renovações fora do prazo e acréscimos de contratos acima dos limites legais.

6.5. A UNIPAMPA executa gestão de serviços e de projetos de TIC, bem como processo de software?

A Instituição executa gestão de projetos de TIC e executa parcialmente gestão de serviços de TIC, sendo necessário desenvolver o processo de gerenciamento do catálogo de serviços e um catálogo publicado e atualizado dos serviços de TIC oferecidos às áreas clientes.

Quanto ao processo de software, foi possível comprovar que é executado, tendo sido apresentados inclusive artefatos que comprovam sua instituição e seu efetivo funcionamento.

7. PONTOS POSITIVOS

Como pontos positivos, além das respostas que foram validadas pela Auditoria, pode-se citar a evolução nos seguintes itens, que na época no questionário eram práticas não adotadas ou adotadas parcialmente:

1. A Instituição realiza avaliação periódica de sistemas de informação.
2. A Instituição realiza avaliação periódica de segurança da informação.
3. A Instituição dispõe de política de controle de acesso à informação e aos recursos e serviços de TI formalmente instituída, como norma de cumprimento obrigatório.
4. O processo para classificação e tratamento de informações está formalmente instituído, como norma de cumprimento obrigatório.
5. A Instituição possui portfólio de projetos de TI.
6. A Instituição executa processo de gerenciamento de projetos de TI.

8. CONCLUSÃO

Foram verificadas as questões mais relevantes no que diz respeito à Governança, ao Planejamento, à Segurança das Informações, aos Contratos de TIC e ao Gerenciamento de serviços e projetos, a fim de chegar às respostas das questões de Auditoria demonstradas no item nº 6 deste Relatório.

Com base nas análises e verificações, pôde-se validar a maioria das respostas aos itens do questionário iGovTI 2014. Das 43 questões selecionadas, apenas 6 não foram validadas e 8 foram consideradas insatisfatórias, apesar de validadas. Isso se deu ao fato da Instituição ter permanecido em situações de prática adotada parcialmente ou prática não adotada.

Salienta-se que 6 questões que representavam práticas que não eram adotadas ou adotadas parcialmente à época do Questionário foram consideradas adotadas integralmente por esta Auditoria.

Entende-se a dificuldade de implantação das ações de TIC em uma Instituição com dez campi, como a UNIPAMPA, mas salienta-se que é justamente essa característica que torna ainda mais necessária a existência de formalização de políticas e de normas de cumprimento obrigatório. Assim a TIC poderá, cada vez mais, auxiliar a Gestão no alcance de seus objetivos.

Bagé, 10 de dezembro de 2015.

GABRIELA GIACOMINI DE MACEDO:01984597000

Digitally signed by GABRIELA GIACOMINI DE MACEDO:01984597000
DN: cn=GABRIELA GIACOMINI DE MACEDO:01984597000, c=BR, o=ICP-Brasil, ou=RFB e-CPF A3, email=gabriela.macedo@unipampa.edu.br
Date: 2015.12.10 17:40:02 -02'00'