Universidade Federal Fluminense

Boletim de Serviço

ANO XLII N.º 106 26/06/2012

ROBERTO DE SOUZA SALLES
Reitor

SIDNEY LUIZ DE MATOS MELLO
Vice – Reitor

ROSANE PIRES FERNANDES
Superintendente de Comunicação Social

SUMÁRIO

ESTE BOLETIM DE SERVIÇO É CONSTITUÍDO DE 043 (QUARENTA E TRÊS) PÁGINAS CONTENDO AS SEGUINTES MATÉRIAS:

ANTONIO LIMA VIANA
Chefe do Serviço de Comunicações Administrativas

LEONARDO VARGAS DA SILVA
Pro Reitor de Administração

SEÇÃO II

Parte 1:

PORTARIA N.º 47.105 de 13 de junho de 2012.

EMENTA: Aprova o Plano Diretor de Tecnologia de Informação e Comunicação –PDTIC – que tem como objetivo orientar as ações institucionais na área de TIC, no período de 2012-2014, para melhor atender as necessidades da UFF, tendo sido elaborado pelo Comitê de Tecnologia da Informação (COTI), instituído pela Portaria n.º 38.355, de 01.07.2008 e reformulado pela Portaria n.º 44.709, de 23/05/2011.

O REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando que um dos grandes desafios atuais da administração pública é melhorar a qualidade da Governança em Tecnologia da Informação e atender às recomendações da Instrução Normativa nº 04/2010; como também às recomendações do Tribunal de Contas da União e do Governo Federal;

Considerando, também, as recomendações das auditorias da Controladoria Geral da União(CGU), ocorridas entre março e abril de 2011, contidas no Relatório de Auditoria Anual de Contas nº 201108970, referente ao processo n.º 23069.002824/2011-96;

Considerando esgotado o período de 11.01.2012 a 29.02.2012 relativo à consulta pública sobre o Plano Diretor de Tecnologia de Informação e Comunicação – PDTIC –, para coleta de críticas e sugestões dos principais gestores desta Universidade;

Considerando, ainda, que este Plano Diretor de Tecnologia de Informação está totalmente alinhado ao Plano de Desenvolvimento Institucional da UFF (PDI), em suas áreas, com respectivos objetivos, estratégias e ações, e será revisto anualmente,

RESOLVE:

1 - **Aprovar o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)** desta Universidade Federal Fluminense, com vigência pelo período de 2012-2014, elaborado pelo Comitê de Tecnologia da Informação (COTI), instituído pela Portaria n.º 38.355,de 01.07.2008 e reformulado pela Portaria n.º 44.709, de 23 de maio de 2011.

2 - **Fazem** parte integrante deste Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), os seguintes documentos:

* Política de Segurança da Informação, aprovado pela portaria nº 47.106, de 13 de junho de 2012,

* Norma de Aquisição de Recursos Computacionais, aprovada pela portaria nº 47.107, de 13 de junho de 2012.

3 - A vigência desta portaria terá início a partir de sua publicação no Boletim de Serviço desta Universidade.

Publique-se, registre-se e cumpra-se.

ROBERTO DE SOUZA SALLES
Reitor
# # # # # #

(Anexo à PORTARIA N.º 47.105 de 13 de junho de 2012.)

SUPERINTENDÊNCIA DE
TECNOLOGIA DA INFORMAÇÃO

Plano Diretor de Tecnologia de Informação e Comunicação – PDTIC

Período de vigência: 2012 – 2014

Marco 2012

Universidade Federal Fluminense

Professor ROBERTO DE SOUZA SALLES REITOR

Professor SIDNEY LUIZ DE MATOS MELLO
VICE-REITOR

Professor RENATO CRESPO PEREIRA
Pró-Reitoria de Graduação

Professor SÉRGIO JOSÉ XAVIER DE MENDONÇA
Pró-Reitoria de Assuntos Estudantis

Professor ANTONIO CLAUDIO LUCAS DA NÓBREGA
Pró-Reitoria de Pesquisa, Pós-Graduação e Inovação

Professor WAINER DA SILVEIRA E SILVA
Pró-Reitoria de Extensão

Professor HEITOR LUIZ SOARES DE MOURA
Pró-Reitoria de Planejamento

JOVINA MARIA DE BARROS BRUNO
Pró-Reitoria de Gestão de Pessoas

LEONARDO VARGAS DA SILVA
Pró-Reitoria de Administração

FERNANDO CESAR CUNHA GONÇALVES
Superintendência de Tecnologia da Informação

Equipe de Trabalho

HÉLCIO DE ALMEIDA ROCHA
Coordenação de Desenvolvimento de Novas Tecnologias

HENRIQUE OSWALDO UZÊDA PEREIRA DE SOUZA
Comissão de Governança e Segurança da Informação

LEONARDO MORAES RIZZO
Coordenação Técnica

THIAGO DIOGO
Coordenação de Desenvolvimento de Sistemas

Integrantes do Comitê de Tecnologia da Informação (COTI)

Colaboradores

LEILA SOARES GONÇALVES, pela STI.
MARCOS DE OLIVEIRA PINTO, representando a Comissão do PDI e PROPLAN.
ROSINA ANGELA PERROTTA DE OLIVEIRA, pela STI.
TERESINHA DIONIZIA MANGOLIN, pela STI.

Histórico de versões

Data	Versão	Descrição	Autor
2009	1.0	Encaminhamento do PDTIC ao COTI.	STI
2010	1.1	Revisão e criação de novo texto para o PDTI.	STI
2011	1.2	Revisão para adequação às recomendações CGU.	STI
2011	2.0	Versão 1 novo PDTIC - reunião 27/04/2011.	STI
2011	2.1	Versão 2 novo PDTIC – reunião 11/08/2011.	STI
2011	2.2	Versão 3 novo PDTIC – reunião 24/08/2011.	STI
2011	2.3	Versão 4 novo PDTIC – reunião 14/09/2011.	STI
2011	2.4	Versão 5 novo PDTIC – reunião 28/09/2011.	STI
2011	2.5	Versão 6 novo PDTIC – reunião 27/10/2011. Justificamos o atraso na entrega dos documentos prometidos ao COTI, até o final de outubro de 2011, em função de fatores sazonais que prejudicaram a consecução de algumas metas planejadas pela Comissão de Governança de TI. Entre esses fatores citamos a greve recente dos servidores federais das IFES; o processo de reestruturação organizacional na área administrativa da UFF (trazendo demandas emergenciais para a gestão da UFF, com prioridades de manutenções nos sistemas internos, no SIAPE e SIAFI); e novas demandas do Projeto REUNI, quando houve um envolvimento maior das equipes de infraestrutura em atividades de planejamento e projeto da instalação de suporte para dados e voz para os novos prédios da UFF. Em paralelo, a partir de nossa participação no II Encontro de TI, pudemos constatar a necessidade urgente de envolver a alta administração da UFF nas decisões sobre a Governança de TI, conforme orientam as entidades de controle interno da administração pública federal (MPOG, SLTI, TCU, SEFTI, e CGU), quanto à aplicação de soluções de TI em benefício ao cidadão brasileiro e a sociedade.	STI
2011	2.7	Versão 7 novo PDTIC submetida à crítica e sugestões da comunidade UFF.	STI
2012	2.8	Versão 8 novo PDTIC já com as atualizações sugeridas pela comunidade UFF e aprovadas pelo COTI, pronta para envio ao reitor.	STI

TERMOS E ABREVIAÇÕES

APF – Administração Pública Federal

BPMN – Business Process Modeling Notation

CGU – Controladoria Geral da União

COTI - Comitê de Tecnologia da Informação da UFF

EGTI – Estratégia Geral de Tecnologia da Informação 2011 – 2012

IN – Instrução Normativa

MPOG – Ministério do Planejamento, Orçamento e Gestão

MPS.BR – Melhoria de Processos do Software Brasileiro

NTI – Núcleo de Tecnologia da Informação e Comunicação da UFF

PDI – Plano de Desenvolvimento Institucional da UFF

PDTIC – Plano Diretor de Tecnologia da Informação da UFF

PMBOK – Project Management of Knowledge

PMO – Project Management Office

SCRUM – Processo de desenvolvimento ágil de forma iterativa e incremental.

SEFTI – Secretaria de Fiscalização de Tecnologia da Informação do TCU

SISP – Sistema de Administração de Recursos de Informação e Informática

SLTI – Secretaria de Logística e Tecnologia da Informação do MPOG

STI – Superintendência de Tecnologia da Informação da UFF

TCU – Tribunal de Contas da União.

TIC – Tecnologias da Informação e Comunicação

UFF – Universidade Federal Fluminense

APRESENTAÇÃO

A Universidade Federal Fluminense (UFF) é uma instituição autárquica ligada ao Ministério da Educação e tem como missão "Gerar avanços científicos, tecnológicos, artísticos e culturais, por meio do ensino, da pesquisa e da extensão, produzindo e socializando conhecimento para formar cidadãos com capacidade de implementar soluções que promovam o desenvolvimento humano sustentável" (Plano de Desenvolvimento Institucional da UFF, 2009-2014).

Foi nessa perspectiva que, a partir de uma reestruturação organizacional iniciada ao final de 2010, a alta administração da UFF explicita a importância da tecnologia da informação para o atendimento da missão e objetivos estratégicos da instituição, e assume o compromisso de criar este Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC). Este Plano Diretor será de vital importância para colocar a UFF entre as melhores Instituições Federais de Ensino Superior, proporcionando à organização alcançar a melhoria da qualidade em seu planejamento e gestão institucional, atingindo posição diferenciada no que se refere à inovação tecnológica e gestão de seu conhecimento interno.

As Tecnologias de Informação e Comunicação (TIC) servem de suporte às atividades acadêmicas e administrativas. No contexto acadêmico, servem como instrumento de pesquisa, coleta e armazenamento da informação, meio de acesso e de difusão da informação, meio de comunicação intra e extramuros e, em especial, entre docentes e discentes. No contexto administrativo, servem como instrumento de automação e racionalização de processos administrativos e de gestão (planejamento, acompanhamento, avaliação e controle), proporcionando uma melhoria na qualidade das decisões tomadas pelos gestores, dando o apoio logístico para que a universidade possa ser mais ágil e eficiente na sua missão, de forma a dar sustentabilidade no desenvolvimento da UFF inovadora.

Cabe ressaltar que ainda há um longo caminho a ser percorrido em termos da gestão eficaz dos recursos de TIC em uma instituição de ensino do porte da UFF. Dessa forma, esperamos que este Plano Diretor seja um elemento catalisador entre o corpo técnico que atua na operação dos recursos de TIC e a Alta Administração da Universidade, com um envolvimento maior nas decisões que envolvem a aplicação de recursos em TIC em todos os municípios da abrangência da UFF, e na priorização das soluções de que devem ser desenvolvidas e implantadas.

A gestão de tecnologia da informação propiciada por este PDTIC pode ser definida como o desenvolvimento de um processo estruturado e controlado, voltado ao alinhamento das necessidades organizacionais, sejam elas no âmbito da competitividade do mercado, sejam na forma de execução de seus processos, com a introdução na UFF, das inovações tecnológicas mapeadas e avaliadas como habilitadoras para a geração dos produtos e servicos, internos ou externos, em atendimento às demandas sociais.

O Plano Diretor de Tecnologia de Informação e Comunicação (PDTIC) que tem como objetivo orientar as ações institucionais na área de TIC no período 2012-2014, para melhor atender às necessidades da UFF está sendo elaborado para posterior submissão a aprovação pelo Comitê de Tecnologia da Informação (COTI), instituído na UFF pela PORTARIA Nº. 38.355 de 01 de julho de 2008, e reformulado a partir de maio de 2011, através da nova PORTARIA nº 44.709 de 23/05/2011 (ANEXO VIII).

Este Plano Diretor está totalmente alinhado ao Plano de Desenvolvimento Institucional da UFF (PDI), em suas áreas, com respectivos objetivos, estratégias e ações, e será revisto anualmente.

SUMÁRIO

1 – INTRODUÇÃO

Um dos grandes desafios atuais da administração pública é melhorar a Governança em Tecnologia da Informação e atender às recomendações da Instrução Normativa 04/2010, às orientações do Tribunal de Contas da União (TCU) e outras recomendações do Governo Federal. Para isso, o caminho mais seguro e eficiente é seguir essas recomendações de boas práticas, que começam com as necessidades de elaboração de um PDTIC e a criação de um Comitê de Tecnologia da Informação.

A utilização das tecnologias de informação e comunicação é questão estratégica para a atual reitoria da UFF, com ações já sendo direcionadas para a melhoria da qualidade das soluções de TI produzidas, introduzindo a Governança de TI com foco em capacitação de servidores em ferramentas de gestão automatizadas (SCRUM, REDMINE, MPS.BR, BPMN, entre outras, iniciadas recentemente) na melhoria dos seus processos internos de gerenciamento de serviço.

Através da propagação do uso destas ferramentas a partir da Superintendência de Tecnologia de Informação (STI), pretende-se viabilizar a transferência desta cultura da governança de TI para os gestores das linhas acadêmicas e administrativas através da introdução de novas práticas gerenciais, com o registro das principais demandas de TI recebidas pela STI e sua gestão conjunta com a administração superior da UFF.

A STI é o órgão responsável por desenvolver, manter e implantar sistemas de informação e demais serviços de comunicação com qualidade e padronização, visando dar suporte à administração da UFF, na evolução de principais processos de ensino, pesquisa, extensão, planejamento e gestão.

A STI gerencia os principais serviços de TIC oferecidos à comunidade UFF, conforme políticas já definidas pela universidade em seu plano principal, o PDI. Para cumprir estes objetivos, a STI mantém e opera uma coleção complexa de equipamentos e sistemas, e conta com uma equipe de pessoas, sob a coordenação do seu Superintendente.

Com a introdução das novas ferramentas automatizadas, que visam melhorar a gerência de serviços e propagar o conhecimento entre seus colaboradores, a STI sinaliza para a urgência de investimento na capacitação de seu pessoal, objetivando organizar a produção das soluções de TI, guiando-se por novas tecnologias, ferramentas e métodos de produção e gestão.

Esta nova filosofia de gestão considerou ainda a adoção do PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK) como metodologia a ser adotada na gerência dos projetos desenvolvidos pela STI. Dessa forma, foi implantado o Escritório de Projetos (Project Management Office - PMO) com o intuito de acompanhar a execução das atividades da STI, otimizando seus resultados no suporte à gerência e qualidade dos projetos em execução.

O Comitê de Tecnologia da Informação (COTI) tem como principais atribuições a elaboração e aprovação deste PDTIC, prestando apoio no estabelecimento de políticas e diretrizes sobre TI, bem como a definição de normas para o uso dos recursos computacionais da Universidade. O COTI é presidido pelo Vice-Reitor, e inclui o Superintendente da STI, dois membros do Instituto de Computação, cinco membros representantes das quatro grandes áreas de conhecimento e dois representantes das unidades do interior.

2 – METODOLOGIA APLICADA

Este PDTIC está sendo atualizado, a partir das visitas e recomendações da última auditoria da Controladoria Geral da União, ocorridas entre março e abri de 2011, cujo resultado final está registrado no RELATÓRIO DE AUDITORIA ANUAL DE CONTAS nº 201108970, referente ao processo 23069.002824/2011-96, sobre o exercício de 2011.

Procurando adequar-se às práticas sugeridas pelo Governo Federal a STI iniciou sua adesão à metodologia de modelagem de processos baseada na notação BPMN, com a utilização da ferramenta BizAgi Process Modeler. Neste sentido, é nossa intenção utilizar a ferramenta para mapear nossos principais processos de trabalho, escolhidos através da utilização desta metodologia de gestão, visando, como resultado final, a geração de serviços de valor ao Reitor, Conselhos Superiores, Pró-reitorias, e Unidades.

Apresentamos, abaixo, o endereço do Portal de Processos onde podem ser visualizados e explorados os primeiros processos organizacionais modelados, sobre as áreas de atuação da STI:

http://www.sti.uff.br/processos/

É importante lembrar que a metodologia de gestão de processos passa a ser adotada objetivando, num primeiro momento, a socialização do conhecimento dos processos organizacionais pelos membros da STI para, em seguida, sensibilizar a alta administração sobre a necessidade de envolvimento total ao processo de gestão da TI, no âmbito dos serviços contratados.

Em função destas novas necessidades de realinhamento de sua gestão foram efetuadas reuniões internas entre os gestores dos principais setores da STI, para um melhor planejamento das ações necessárias ao atendimento das recomendações recebidas pelo órgão de controle externo.

Internamente, entre os meses de março e agosto de 2011, recebemos a demanda emergencial da alta administração da UFF no que se refere ao processo de reestruturação organizacional da área administrativa da UFF iniciado em novembro de 2010, e culminando com a criação de novas pró-reitorias e superintendências. Tal demanda trouxe necessidades de adequação dos sistemas internos (acadêmicos e administrativos) ainda em processo de adaptação. Durante esse mesmo período foram realizadas reuniões com estas novas pró-reitorias para conhecimento de suas necessidades por soluções de TIC.

O Comitê de Tecnologia da Informação (COTI), como instância responsável pela aprovação deste PDTIC, e atuando de forma consultiva e normativa sobre o uso dos recursos computacionais da UFF, também é responsável pelo encaminhamento deste documento à aprovação do reitor e conselhos superiores da UFF.

3 – DOCUMENTOS DE REFERÊNCIA

Segundo a Instrução Normativa SLTI nº 04/2010 em seu art. 2°, inciso XXII, o Plano Diretor de Tecnologia da Informação – PDTI é o instrumento de planejamento de TI a ser utilizado no âmbito da APF. Ainda segundo a IN nº 04/2010, um PDTI é um “instrumento de diagnóstico, planejamento e gestão dos recursos e processos de Tecnologia da Informação que visa atender às necessidades tecnológicas e de informação de um órgão ou entidade para um determinado período”.

Este PDTIC tem como referência principal, para o norteamento de suas ações e estratégias o PDI da UFF atualmente em vigor.

Em relação à sua forma, este PDTIC tem a sua estrutura baseada no modelo de Plano Diretor de Tecnologia da Informação, referência 2011-2012, elaborado pelo MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, através de sua Secretaria de Logística e Tecnologia da Informação – SLTI integrante da comunidade do Sistema de Administração de Recursos de Informação e Informática (SISP).

Como principais referenciais teóricos iniciamos o alinhamento com as diretrizes do Governo Federal, estabelecidas nos documentos Estratégia Geral de Tecnologia da Informação (EGTI) 2011-2012 e pelo Guia de Boas Práticas em Contratação de Soluções de TI, V 1.0, ambos elaborados pelo MINISTÉRIO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO, através de sua Secretaria de Logística e Tecnologia da Informação – SLTI.

4 – PRINCÍPIOS E DIRETRIZES

O PDTIC escolheu como princípios e diretrizes, os objetivos estratégicos abaixo, que serão os principais desafios para o desenvolvimento institucional da UFF para os próximos anos, nos campos do ensino, pesquisa, extensão e administração, contando com a criação da função de Governança de TI com respaldo da alta administração da UFF.

• Estabelecer um modelo de Governança de TI na Universidade totalmente alinhado ao PDI, em suas áreas estratégicas e respectivos objetivos, estratégias e ações onde a aplicação das TI produza os resultados organizacionais planejados.

• Manter o alinhamento (parcial e/ou total) com as diretrizes da Administração Pública Federal (APF), estabelecidas pelos órgãos de controle interno (MPOG, SLTI, TCU, SEFTI, e CGU), no que se refere à aplicação das soluções de TI.

• Desenvolver a Central de Atendimento para prestar um serviço de qualidade excelente aos clientes da UFF (segmentos acadêmicos e administrativos), para melhoria do processo de comunicação da STI.

• Fomentar ações de integração entre os sistemas corporativos para melhoria da qualidade das informações gerenciais e estratégicas necessárias.

• Garantir a evolução da capacidade técnica da STI para proporcionar infraestrutura de TI em resposta às demandas internas e externas sempre crescentes.

5 – ESTRUTURA ORGANIZACIONAL DA UNIDADE DE TI

A Superintendência de Tecnologia de Informação (STI) é o órgão estratégico na Universidade Federal Fluminense responsável por prover de serviços e soluções de tecnologia da informação as comunidades interna (composta por cerca de 50.000 pessoas entre alunos, professores, técnicos e gestores institucionais) e externa, (representada pela sociedade brasileira, como um todo e diversas instituições internacionais).

Atravessando uma recente reestruturação organizacional, através do que menciona a PORTARIA N.º 44.338 de 31 de março de 2011 (ANEXO IX), a STI também desenvolve ações de alinhamento aos padrões determinados pela Administração Pública Federal, passando a utilizar a função de Governança em TI para alcançar melhores resultados nas soluções de TI produzidas e proporcionar transparência ao público brasileiro sobre o andamento e avaliação de seus projetos.

Seus principais serviços estão relacionados às áreas de manutenção da rede UFF; segurança da informação, administração de sistemas de informações, manutenção de e-mails, criação e manutenção de bases de dados, desenvolvimento de portais, serviços de videoconferência, administração de rede de telefonia, administração de laboratórios de graduação, entre outros.

A nova estrutura organizacional é representada pela sua alta administração, mostrada na pela figura abaixo, com breve descrição das principais atribuições destes órgãos. Cabe ressaltar a mudança estratégica na posição da STI, que passa a estar ligada diretamente à Reitoria da UFF.

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO – STI

Planejar, dirigir, coordenar e supervisionar as atividades da STI, respeitadas as políticas e as diretrizes estabelecidas pelo Reitor, bem como praticar os demais atos necessários ao desempenho de suas atribuições.

GERÊNCIA OPERACIONAL FINANCEIRA – GOF/STI

Manter cadastro atualizado dos contratos e convênios firmados, bem como a situação administrativo-financeira de cada um.

GERÊNCIA DE DESENVOLVIMENTO INSTITUCIONAL – GDI/STI

Coordenar, organizar planos, programas e projetos de treinamento para capacitação de recursos humanos.

GERÊNCIA DE RELACIONAMENTO EXTERNO – GRE/STI

Promover eventos técnicos como seminários, simpósios, encontros, reuniões, etc. sobre temas estratégicos na área.

COMISSÃO DE GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO – CGSI/GDI

Analisar, desenvolver, implantar e normatizar políticas de governança de TI e segurança da informação.

COMISSÃO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIAS – CDNT/GDI

Desenvolver e consolidar na STI a capacidade de catalisar e implementar estudos, pesquisas e aplicações relacionadas à Tecnologia da Informação e Comunicação.

CENTRAL DE ATENDIMENTO – CA/STI

Prover suporte de 1º e 2º níveis.
Centralizar os atendimentos, direcionando-os às áreas competentes.
Melhorar a gestão da STI com a criação de uma base sobre o conhecimento interno.

COORDENAÇÃO TÉCNICA – CTE/STI

Planejar, divulgar, coordenar e supervisionar as atividades da Coordenação de acordo com as diretrizes da Superintendência.

COORDENAÇÃO DE DESENVOLVIMENTO DE SISTEMAS – CDS/STI

Planejar, assessorar e supervisionar os órgãos superiores quanto a política e diretrizes de desenvolvimento de sistemas de informação.

A força de trabalho dos servidores públicos lotados na STI contempla um total de 82 servidores, sendo que oito servidores estão cedidos a outros órgãos da UFF, e um servidor encontra-se em licença sem vencimentos. Em relação ao nível de formação dos servidores 45 possuem formação superior, 30 possuem formação em nível médio e 5 possuem formação no nível do ensino fundamental. Quando quantificados os totais de servidores por cargos observamos os seguintes totais, conforme quadro abaixo:

Cargo do servidor	Totais	Cedidos
Analistas de TI	35	6
Técnicos de TI	23	1
Auxiliar Administrativo	7	2
Telefonista	5	
Assistente Administrativo	4	
Assistente em TI	2	
Bibliotecário	1	
Administrador de Edifícios	1	
Técnico em Refrigeração	1	
Técnico em Secretariado	1	
Técnico em Eletrotécnica	1	
Contínuo	1	
Totais	**82**	**9**

Fonte: Folha de Pagamento SIAPE – Março de 2012

Além da força de trabalho dos servidores públicos mencionada no quadro acima, a STI para dar continuidade em seu atendimento às demandas crescentes da UFF, conta com a participação de alunos de graduação, que atuam como bolsistas, e que prestam apoio às áreas de desenvolvimento de portais e softwares corporativos, infraestrutura, e atendimento ao cliente, conforme quadro abaixo. Vale ressaltar que esta participação de alunos em atividades profissionais foi conseguida através de parcerias firmadas com o Instituto de Computação da UFF, Escola de Engenharia da UFF, e Instituto de Arte e Comunicação Social da UFF.

Cargo do aluno	Totais	Cedidos
Analista de Sistema	7	
Desenvolvedor de Software	24	
Analista de Infraestrutura	5	
Analista de Mídia	6	
Atendente Central de Atendimento.	5	

Fonte: Agosto de 2011

Em relação aos serviços de TI contratados através de licitação pública, a STI informa que fiscaliza os serviços relacionados ao contrato nº. 064/2010-PG, e processo 23069.051093/2009-98, que podem ser consultados pelos interessados em acompanhar as atividades desempenhadas pelo fornecedor das soluções de TI contratadas.

6 – REFERENCIAL ESTRATÉGICO DE TI

6.1 – MISSÃO

A Superintendência de Tecnologia da Informação – STI tem por finalidade básica realizar a gestão de infraestrutura de software e hardware da universidade, além de planejar e executar a política de informática da universidade. Também faz parte de sua missão pesquisar, desenvolver, executar e participar de projetos em Tecnologia da Informação e serviços de informática tanto internamente, nos diversos Campi que compõem a UFF, como em parcerias com Municípios e Estados, além da captação de recursos através de projetos, consultoria e serviços em TI.

6.2 – VISÃO

Desenvolver e capacitar os recursos humanos da STI com o objetivo de organizar a produção de soluções de TI, em atendimento às demandas das áreas estratégicas do PDI, sempre com alinhamento às novas tecnologias, ferramentas e métodos.

6.3 – VALORES

- Alinhamento Estratégico
- Respeito
- Comprometimento
- Ética
- Excelência em TI
- Trabalho em equipe
- Foco no cliente

6.4 – OBJETIVOS ESTRATÉGICOS DE TI

A distribuição geográfica da UFF obriga o uso intensivo de tecnologias de comunicação. A UFF tem sua sede em Niterói, e está presente em outros 16 municípios do estado do Rio de Janeiro e um no estado do Pará. Adicionalmente, suas instalações em Niterói estão distribuídas por 18 imóveis distintos em vários bairros da cidade, envolvendo 3 campi e 15 unidades dispersas. Nos 16 municípios do estado a UFF está presente com 4 pólos universitários e 12 unidades isoladas.

A Universidade desenvolve as mais diversas atividades de ensino, pesquisa e extensão, mediante 102 cursos de graduação presenciais (sendo 33 no interior do estado), 5 cursos de graduação a distância (em 27 municípios do estado), 1 curso sequencial a distancia, 78 cursos de pós-graduação stricto sensu, 132 cursos de pós-graduação lato sensu, 2 cursos de pós-graduação à distância, 90 cursos de extensão, o Hospital Universitário Antônio Pedro, 27 Bibliotecas, o Colégio Universitário e a Creche. Para desenvolver esta atividade intelectual, conta com a produção de 96 departamentos de ensino, que integram a estrutura das unidades universitárias e atuam na gestão acadêmica para o bom andamento dos cursos. Como consequência, a infraestrutura de TIC da UFF depende em grande parte de boas condições de comunicação entre estes locais dispersados, e a STI opera uma grande rede de comunicação em Niterói – RedeUFF (ANEXO III), estendida através de diversos enlaces de comunicação entre Niterói e suas unidades em outras cidades.

Os laboratórios de graduação são vinculados à Pró-reitoria de Graduação (PROGRAD) e criados para atender sugestões contidas nas avaliações periódicas realizadas pelo MEC, sobre as condições físicas dos laboratórios para que os diversos cursos de graduação da UFF oferecidos à comunidade tenham condições plenas para aprimorar constantemente seus currículos.

Devido a seu caráter específico, e as fontes externas à UFF dos recursos aplicados em sua montagem, os laboratórios de pesquisa que fazem uso de TIC não são contemplados por este PDTIC no que diz respeito a quaisquer restrições de configuração de *hardware ou software*.

Em resumo, para o atendimento das necessidades da instituição e das normativas do governo federal e para uma maior organização em direção à Governança de TI, listamos abaixo os principais objetivos estratégicos deste plano:

- Sensibilizar a alta administração para importância das decisões relacionadas à governança de TI, principalmente, sobre a priorização de desenvolvimento das soluções e investimentos em TI;

- Desenvolver, entregar e manter sistemas de informação que sejam confiáveis, seguros e eficazes;

- Evoluir os sistemas para garantir o suporte às mais novas tecnologias disponíveis no mercado de TI;

- Fortalecer o relacionamento com o cliente final, atendendo e comunicando com qualidade nossos usuários;

- Expandir parcerias com empresas privadas para soluções de TI para a UFF;

- Apoiar nossos profissionais na sua evolução pessoal e técnica, sendo justo na cobrança e reconhecimento;

- Implantar uma política composta por padrões e normas de desenvolvimento e utilização dos sistemas de informação da UFF;

- Aprimorar as políticas de uso e segurança dos dados da UFF.

6.5 – ANÁLISE SWOT DA TI ORGANIZACIONAL

A análise SWOT é uma ferramenta utilizada para análise de cenários, interno e externo, usado como base para gestão e planejamento estratégico de uma organização. É uma metodologia que possibilita verificar e avaliar os fatores intervenientes para um posicionamento estratégico da Unidade de TI no ambiente em questão, a nossa Universidade Federal Fluminense.

Existem diversas técnicas de levantamento desses fatores, e a técnica denominada SWOT (strengths, weaknesses, opportunities and threats), que pode ser traduzida por “forças (pontos fortes)” e “fraquezas (pontos a serem melhorados)”, “oportunidades” e “ameaças”. As forças e as fraquezas podem ser controladas pelo indivíduo, já as oportunidades e ameaças são antecipações do futuro e estão relacionadas a fatores externos. A matriz SWOT é muito utilizada em cenários que estão em mudança, é de utilização simples e muito utilizada por gestores de TI.

A STI em seu novo modelo organizacional, inicia a adesão a essa metodologia, com intenção de se tornar mais competitiva sobre o desenvolvimento e a gestão de soluções de TI. Neste sentido, a elaboração da análise SWOT permitirá que se faça um inventário das principais forças e fraquezas internas, para estabelecer melhores estratégias, e assim, fazer melhor uso das oportunidades se protegendo das ameaças, levando a STI e UFF a buscarem e alcançarem a inovação, nas questões sobre a Governança de TI e produção de conhecimento, respectivamente.

A princípio iremos considerar as variáveis abaixo:

Forças	Variáveis
Equipe bem treinada.	Cultura da organização: chave do sucesso
Administradores experientes	Conhecem o negócio
Sinergia entre a equipe de funcionários	Todos demonstram comprometimento
Equipe motivada.	Todos demonstram motivação
Fraquezas	Variáveis
Entrega Serviços	Ruim - banda de acesso está sendo insuficiente
Operação	Mesmo motivados os funcionário não estão sendo eficientes por conta do maquinário defasado
Instalações	As instalações estão em um estado muito ruim, demonstrando infiltrações.

Oportunidades	Variáveis
Capacitações oferecidas	Poucos concorrentes.
Investimentos em infraestrutura	Investimento do governo nas universidades.
Maior comprometimento da alta administração com a TI.	Condições e boas oportunidades para a área de TI.
Aumento da demanda de Serviços	A demanda sempre crescente.
Ameaças	Variáveis
Restrição orçamentária.	Cortes no orçamento comprometendo novas demandas.
Aumento das responsabilidades e atribuições do setor sem aumento da quantidade de funcionários.	A falta de estrutura interna para aumentar a eficácia da operação pode prejudicar alguns usuários.

Como sugestão a STI pretende, com a força política que vem recebendo da alta administração da UFF, fazer valer a força e sinergia existente entre suas áreas internas para atingir seus objetivos principais ocasionando, como consequência, apoiar a UFF a cumprir sua missão institucional, onde cada unidade deve ser considerada parte de um processo maior.

Com o objetivo de proporcionar a sinergia acima representada, planejamos a elaboração de questionários para aplicação junto aos servidores e colaboradores da STI, para identificação de como enxergam seus ambientes (interno e externo), bem como sobre seus conhecimentos em relação às boas práticas internacionais de TI, como ITIL, COBIT e Gestão de Processos, que muito têm ajudado as organizações a melhorar os seus serviços e sua gestão organizacional.

7 – RESULTADOS DO PDTI ANTERIOR

Objetivamos continuar o desenvolvimento iniciado em 2010, visando à modernização da gestão dos recursos de TIC, conforme o identificado no cenário educacional atual, onde estes recursos podem proporcionar novas formas de criar novos serviços ligados à pesquisa, ensino e gestão institucional. Ao mesmo tempo, alinhados aos objetivos planejados para o PDI e REUNI, pretendemos uma atualização de conhecimentos sobre a gestão de TIC na UFF, permitindo o seu desenvolvimento e sua consolidação como referência nacional em ensino, pesquisa e extensão, possibilitando o reconhecimento da UFF como instituição de qualidade e excelência em gestão administrativa. Ao mesmo tempo, o governo federal vem introduzindo novos conceitos – como Governo eletrônico e Governança de TI – que pressupõe uma necessidade de atualização pelo corpo de servidores técnicos da STI, para introduzir estes conceitos na UFF.

No último ano, a STI atingiu alguns dos objetivos propostos inicialmente (ANEXO I).

8 – ALINHAMENTO COM A ESTRATÉGIA DA ORGANIZAÇÃO

As ações estratégicas deste PDTIC estão alinhadas ao PDI vigente, nas suas principais áreas de Graduação e Pós-graduação; Pesquisa e Extensão; Gestão de Pessoas; Planejamento e Gestão e Interiorização. Através de um planejamento de TI, apoiado por um processo gerencial administrativo e anual de identificação das principais prioridades do PDI, são definidas as metas do PDTIC necessárias para apoiar a instituição na execução de seu plano de negócios, em apoio ao alcance de seus objetivos organizacionais, conforme preconiza a Instrução Normativa 04/2010.

A STI é chamada a participar de reunião da Comissão de Metas do PDI, onde colabora na elaboração de planos orçamentários sobre aquisição de hardware, software e demais recursos computacionais, para determinado ano.

Em reuniões anteriores, foi recomendado pelo COTI, uma nova linha de ação, onde a STI deve participar mais ativamente, em função do grande aumento das demandas recebidas, face o grande número de prédios que vem sendo construídos, em função das metas do Projeto REUNI, com tarefas adicionais de cabeamento e configuração das novas estruturas na RedeUFF, para proporcionar melhoria do atendimento aos alunos, aos novos cursos, departamentos de ensino e unidades universitárias.

9 – INVENTÁRIO DE NECESSIDADES

9.1 – NECESSIDADES IDENTIFICADAS

A STI elaborou uma nova forma de documentação onde registra as necessidades de soluções de TI para os diversos órgãos da UFF. Nesse trabalho foi feita uma análise criteriosa para adequar cada solução de TI às áreas, objetivos, estratégias e ações do PDI da UFF que está válido para o período de 2009 a 2012. Nessa documentação são registrados (para as áreas de governança de TI, sistemas de informação, suporte técnico e novas tecnologias) os nomes dos projetos, sua descrição sucinta, o principal cliente, a necessidade atual do cliente, o valor que agrega à UFF, o status atual, os produtos entregáveis para os próximos 12 meses, a posição que o projeto espera atingir em 2014 e a vinculação do projeto ao PDI.

Com o objetivo de alinhamento das necessidades da UFF com as atividades da STI, utilizamos um formulário para consulta à Comunidade UFF no próprio site da STI, disponível em http://www.sti.uff.br/atendimento-ao-usuário .

9.2 – CRITÉRIOS DE PRIORIZAÇÃO

Os critérios iniciais de priorização das necessidades serão baseados na própria priorização do Plano de Desenvolvimento Institucional (PDI) da UFF.

Com base nessa priorização do PDI, definiremos uma matriz de Gravidade, Urgência e Tendência (GUT) para cada demanda, definindo dessa forma a prioridade da STI.

10 – PLANO DE METAS E AÇÕES

O plano de metas e ações da STI foi desenvolvido com base em uma análise inicial do PDI vigente e o desdobramento de suas metas e ações, em projetos de TI (ANEXO II), também disponível em http://www.sti.uff.br/governanca-de-ti/documentos-uff .

11 – PLANO DE GESTÃO DE PESSOAS

O objetivo principal da capacitação da STI é desenvolver a habilidade da produção de soluções criativas e úteis, através da utilização das tecnologias mais inovadoras do mercado.

Dessa forma, a STI investe em capacitação de novos membros bem como, na manutenção e evolução dos membros que já fazem parte do grupo.

Os principais objetivos da Capacitação da STI são:

- Desenvolver pessoalmente cada membro da STI;
- Capacitar cada membro a desenvolver soluções e a trabalhar em equipe;
- Selecionar bolsistas já capacitados;
- Divulgar e manter o conhecimento dos processos de trabalho da STI;
- Divulgar o nome e a marca da STI através da prestação de um serviço de qualidade;

A **capacitação interna** da STI está organizada da seguinte forma:

- Cursos

o Capacitação de novos estagiários com duração de 1 a 2 meses.

- Workshops

o Encontros técnicos das equipes com objetivo de trocar experiências e conhecimentos sobre as tecnologias e práticas utilizadas na STI. A tendência é que seja um encontro rápido (informal) para troca de conhecimento.

- Projetos internos

o Desenvolvimento de ferramentas e soluções internas para solução de problemas comuns a todos os projetos.

O planejamento da STI para a capacitação externa envolverá a participação em cursos, seminários, eventos, workshops e treinamentos nas seguintes áreas de atuação/temas:

- Governança de TI
- Gestão de Processos;
- Gestão de Projetos baseado no PMBOK e MPS.BR
- Gestão de TI baseado no COBIT
- Desenvolvimento ágil de software
- Segurança da informação
- Gestão de serviços de TI com base no ITIL
- Infraestrutura de redes e internet
- Difusão multimídia

A STI participa de fórum de discussão (CGTIC da ANDIFES) sobre o levantamento da demanda e ingresso de novos servidores na área de TIC.

12 – PLANO DE INVESTIMENTOS EM SERVIÇOS E EQUIPAMENTOS (proposta orçamentária)

Atualmente o orçamento da STI está vinculado ao PDI da UFF e os custos fixos da área de TI, definidos no orçamento geral da UFF.

13 – PLANO DE GESTÃO DE RISCOS

Como necessidade de introdução da gerência de riscos no setor de Governança de TI da STI, iniciou-se um trabalho de identificação de riscos visando, posteriormente, uma análise qualitativa e quantitativa, com planos de contingências prontos para responder à incidência do risco.

Wrigth (2004) ao analisar 23 tipos de riscos associados à contratação de serviços de TI, concluiu que os mais importantes foram riscos de segurança a informação; riscos de dependência do fornecedor e riscos de disputa legal.

Na atual gestão da STI, ao iniciar esta nova ferramenta de gestão, os principais riscos para a comunidade acadêmica e gestão da UFF são:

- Descontinuidade de investimento em TI;
- Falta de investimento em manutenção de infraestrutura e atualização tecnológica;
- Falta de investimento / capacitação em pessoal de infraestrutura e sistemas;

- Falta de investimentos em comunicação;
- Integridade de dados;
- Segurança da informação;
- Disponibilidade da informação;
- Desempenho dos serviços de TI.

São utilizados nesta gestão, os artefatos de software automatizado, nova central de atendimento para melhorar a qualidade da informação fornecida, entre outras ações.

As funções de monitoramento e controle comporão o processo de gerenciamento de riscos, em uma fase mais avançada da implantação da gerência de riscos, inclusive adotando práticas de priorização dos riscos como a Matriz Gravidade, Urgência e Tendência (GUT).

14 – PROCESSO DE REVISÃO DO PDTIC

Este PDTIC será revisto, anualmente, sincronizado às atualizações do PDI, sendo submetido à discussão e aprovação pelo COTI, para posterior encaminhamento aos conselhos superiores da UFF, com publicação de portaria do reitor, específica para validar a nova versão do PDTIC.

15 – FATORES CRÍTICOS DE SUCESSO

Os fatores críticos de sucesso são os pontos chave que definem o sucesso ou o fracasso de um objetivo definido por um planejamento de determinada organização. Estes fatores precisam ser encontrados pelo estudo sobre os próprios objetivos, derivados deles, e tomados como condições fundamentais a serem cumpridas para que a instituição sobreviva e tenha sucesso na sua área. Quando bem definidos, os fatores críticos de sucesso se tornam um ponto de referência para toda a organização em suas atividades voltadas para a sua missão.

Fatores Críticos de Sucesso também são fatores que definem as principais orientações que a gestão deve seguir na implementação de um verdadeiro controle sobre os processos de gestão da tecnologia da informação que, na Universidade Federal Fluminense, que relacionamos abaixo:

- Dar suporte à UFF para o desempenho qualitativo de suas atividades de ensino, pesquisa, extensão e administração;

- Garantir a qualidade dos serviços de TI contratados, para proporcionar valor e resultados positivos à comunidade acadêmica da UFF, cidadãos e a sociedade como um todo;

- Tornar o processo de implantação do PDTIC um compromisso institucional da alta administração da UFF, devendo ser conduzido de forma integrada aos processos que gerem valor para a UFF e sociedade;

- Garantir que as contratações de serviços e produtos de TI na UFF sejam fundamentadas em análise e em parecer das áreas de tecnologia da informação, em consonância com as diretrizes do governo federal (Guia de Boas Praticas em Contratação de Soluções de TI V 1.0 da Secretaria de Logística e Tecnologia da Informação do MPOG);

- Compor um quadro de competências de TI com as especialidades necessárias para atender às ações e aos projetos definidos no PDTI;

- Garantir recursos humanos, orçamentários e financeiros para a execução das ações e dos projetos do PDTI;

- Institucionalizar o modelo de governança de TI, proposto neste PDTI;

• Institucionalizar a participação de servidores da STI em fóruns decisórios da UFF, visando consolidar o papel da tecnologia da informação na gestão estratégica e garantir o alinhamento da TI às estratégias organizacionais;

• Descrever o processo conceitual referente às necessidades de informação, antes de iniciar sua automação;

Abaixo apresentamos os fatores críticos de sucesso por temas específicos de gestão de TI para apreciação e aprovação do grupo:

Tema1: Análise SWOT com colaboradores da STI

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • Equipe bem treinada. • Sinergia entre a equipe de funcionários dentro de um mesmo setor da STI. • Equipe motivada.	Oportunidades: • Maior comprometimento da alta administração com a TI. • Realização de capacitações oferecidas pela Instituição. • Melhora do planejamento com a elaboração do PDTIC. • Novos serviços estratégicos (vídeo vigilância e telefonia). • Expansão da universidade (maiores recursos para a STI). • Automação de processos e serviços da instituição utilizando a TI. • Sistema integrado para agilizar a tomada de decisão. • Interação com outras universidades
Pontos Fracos: • Falha em gerenciamento de projetos e planejamento. • Espaço físico limitado. • Falta de integração entre os diferentes setores da STI. • Escassez de recursos humanos para atender às demandas institucionais. • Falta de documentação, processos e compartilhamento de informações. • Fraca divulgação dos serviços realizados. • Ausência de plano de continuidade de negócio. • Funcionários exercendo cargos de supervisão dos setores sem receberem remuneração por cargos de confiança.	Ameaças: • Restrição orçamentária. • Aumento das responsabilidades e atribuições do setor sem aumento da quantidade de funcionários. • Falta de planejamento dos demais órgãos. • Falta de informações sobre projetos externos. • Acesso não autorizado aos dados institucionais. • Fraca segurança física dos equipamentos (fibra, racks, switches) na Instituição. • Mudança na alta administração da Instituição. • Aquisição de equipamentos de TI sem homologação da STI. • Falta de padronização e integração de processos dentro da Instituição.

Tema 2: Gestão de Pessoas

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • Apoio da DRH para obtenção de treinamentos. • Quadro grande de colaboradores. • Treinamento eficiente para usuários nos sistemas desenvolvidos pela STI. • Tomada de decisão colegiada. • Equipe alinhada e confiável.	Oportunidades: • Orçamento para treinamento planejado e mantido. • Necessidade de cumprir requisitos com ITIL, CobiT e Processos. • Resoluções. • Reestruturação Organizacional da STI.
Pontos Fracos: • Não possui um programa de treinamento direcionado a equipe de TI. • Não possui visão de gestão por processo. • Dificuldade em formalizar processos. • Não consegue aplicar o PDCA. • Falta de estrutura organizacional do Departamento adequada à realidade. • Falta de desenvolvimento gerencial.	Ameaças: • Maioria dos treinamentos é fora de Niterói. • Burocracia no processo de solicitação de treinamento. • Demais áreas não respeitam os poucos processos internos. • Gestão de problemas das outras áreas. • Credibilidade da STI. • Falta de alinhamento com demais áreas.

Tema 3: Governança de TI

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • A implantação do portal corporativo como ambiente de integração e colaboração de toda STI envolvendo alguns gestores dos outros Departamentos. • Fortalecer a implantação do processo de engenharia de software.	Oportunidades: • Contratação de serviços especializados. • O envolvimento de gestores de outros Departamentos ajudou na manutenção do portal corporativo. • Apoiar a implantação/aderência do processo de engenharia de software para todo o departamento.
Pontos Fracos: • Falta de conhecimento sobre o que é Governança de TI e a implantação de seus princípios. • STI não é vista como setor estratégico. • Falta apoio aos processos implantados internamente no próprio departamento, prejudicando a implantação/definição da governança, definição das regras, políticas, diretrizes responsáveis/papéis.	Ameaças: • Falta de comprometimento e credibilidade das demais áreas. • Falta de alinhamento com demais áreas.

Tema 4: Gerência de Projetos de TI

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • Na área de desenvolvimento e suporte existem iniciativas de gerenciamento. • Possuem ferramentas de apoio à gerência de projeto. • A iniciativa de gerenciamento de projeto em 2011 na Divisão de Análise teve como premissa a definição e implantação do processo de engenharia de software baseado na metodologia SCRUM.	Oportunidades: • Contratação de serviços especializados.
Pontos Fracos: • Pouco conhecimento da metodologia PMBOK. • Devido a sobrecarga de trabalho, as atividades de gerenciamento são poucas, sem estrutura e ineficientes. • Falta administração por projetos. • Problemas de comunicação interna e externa e falta de integração entre as equipes.	Ameaças: • Pouco comprometimento das demais áreas, externas à TI. • A qualidade das informações é duvidosa na maior parte das vezes. • Dificuldade de definição dos clientes / responsáveis pelos projetos (stakeholders) e das suas necessidades de forma formal, existe muita informalidade por falta da aderência /comprometimento com o processo.

Tema 5: Gerenciamento de Serviços de TI

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • Existe uma estrutura de Help-Desk, mas com atuação limitada.	Oportunidades: • Contratação de serviços especializados. • Apoiar/revitalizar a implantação/aderência do processo de engenharia de software para todo o departamento.
Pontos Fracos: • Pouco conhecimento da biblioteca da ITIL. • Processos internos definidos, mas não difundidos. • As atividades de gerenciamento se resumem monitorar a operação, principalmente do Datacenter. • Falta de uma ferramenta de atendimento melhor / mais abrangente com indicadores.	Ameaças: • Dificuldade de apresentar para a administração superior indicadores precisos que direcionem outras ações.

Tema 6: Desenvolvimento de Sistemas

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • A equipe é composta por colaboradores, em sua maioria de ótima capacidade técnica. • Possui os ambientes de desenvolvimento, homologação e produção segregados. • Possui uma ferramenta de controle de versão. • Os novos sistemas são desenvolvidos em JAVA. • A documentação dos sistemas está baseada em UML; • Padrão para desenvolvimento Java (tjpr-framework), os servidores de aplicação JEE (JBoss) em cluster, as ferramentas de gerenciamento de dependências, configuração da implementação e ciclo dos projetos (Maven2), de integração contínua e disponibilização nos ambientes de desenvolvimento, teste e produção com liberação de versões e testes automatizados (Hudson), além da ferramenta de controle de versão (Subversion), sendo que todas são open source.	Oportunidades: • As habilidades de analistas de negócio têm surgido naturalmente. • Existe um projeto de reestruturação da área. • Contratação de serviços especializados. • Apoiar/revitalizar a implantação/aderência do processo de engenharia de software para todo o departamento.
Pontos Fracos: • Existem vários módulos de sistemas em desenvolvimento e/ou manutenção. • Falta de aderência do departamento em geral com o processo de desenvolvimento de software implantado. Utilização de, pelo menos, três linguagens de programação diferentes. • Utilizam mais de dois bancos de dados diferentes.	Ameaças: • Não consegue organizar um processo de priorização de atividades. • Geração de demanda de sistemas é descontrolada pelos usuários. • A atual estrutura está sobrecarregando a gestão. • Continuar sem aderência/comprometimento ao processo de desenvolvimento de software.

Tema 7: Segurança da Informação

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • As áreas desenvolvem uma avaliação e tratamento mínimo de risco, com foco em sistemas e segurança de rede.	Oportunidades: • Contratação de serviços especializados.
Pontos Fracos: • Existem iniciativas descentralizadas de segurança da informação; • Estrutura de segurança da informação ainda em definição e implantação; • Existem poucas ferramentas de controle e inexistência de normas.	Ameaças: • Se os usuários da STI questionarem as regras colocadas. • O ambiente é suscetível a graves incidentes. • A falta de alinhamento com as demais áreas dificulta as atividades de segurança.

Tema 8: Gestão de Infraestrutura

FATORES CRÍTICOS

Ambiente interno	Ambiente externo
Pontos fortes: • Já utilizam da tecnologia de virtualização com muito sucesso. • A infraestrutura física de rede é de ótima qualidade e muito bem gerenciada. • Utilizam o gerenciamento dos recursos do Datacenter com MRTG e NAGIOS, gerando um Dashboard de boa qualidade. • Suporte técnico de 1º. Nível com atendentes também distribuído pelas regionais.	Oportunidades: • Contratação de serviços especializados.
Pontos Fracos: • O ambiente do Datacenter não segue as boas práticas e normas internacionais. • Não possui repressão de fogo com gás inerte no Datacenter. • Não adotam a ITIL, deixando assim uma grande lacuna no processo de atendimento.	Ameaças: • A política de atualização de hardware é baseada na demanda. • A STI como um todo não segue as regras e normas estabelecidas nas políticas de segurança.

16 – CONCLUSÃO

Este PDTIC é a primeira versão atualizada após a reestruturação administrativa ocorrida na UFF, onde a nova STI passa a ser subordinada diretamente ao Gabinete do Reitor (GAR), ao mesmo tempo em que inicia o seu planejamento da Governança de TI a partir de 2011.

Os crescentes controles dos órgãos da administração pública federal, especialmente o TCU, que desenvolveu pesquisas sobre a atuação da alta administração na implantação da Governança de TI, foram fundamentais para identificar o enorme volume de recursos financeiros aplicados em tecnologia da informação pela administração pública federal (só no último ano, a área de TI respondeu por R$ 3,8 bilhões de reais).

Tal volume de recursos traz enormes preocupações aos gestores no sentido de acompanhar e conhecer bem suas necessidades em TI, para evitar gastos desnecessários dos recursos públicos. Segundo o TCU – como objetivo maior da IN 04/2010 – é importante que cada real gasto com TI esteja totalmente associado a um benefício concreto aos cidadãos e, para que a administração possa garantir esta relação é necessário um planejamento bem executado, com monitoração constante de metas, aplicações financeiras, e resultados ao cliente. Para ilustrar a preocupação dos órgãos de controle interno informamos, no quadro abaixo, alguns indicadores coletados em pesquisa realizada em 2007:

Deficiências em Governança de TI
51% NÃO alocam gastos de TI de acordo com planejamento
51% NÃO seguem metodologia de desenvolvimento de sistemas
57% NÃO têm carreira específica para TI
59% NÃO têm planejamento estratégico em vigor
64% NÃO têm política de segurança da informação
75% NÃO fazem análise de riscos de TI
80% NÃO fazem classificação da informação
88% NÃO têm plano de continuidade de negócios

Fonte TCU – pesquisa de 2007

No ano de 2010 o TCU convidou, para alguns eventos em Brasília, todos os representantes máximos da administração pública federal para conscientizá-los sobre a importância de sua participação na implantação da Governança de TI em cada um dos órgãos sob sua gestão. Na ocasião, foram informados resultados de pesquisas realizadas sobre a participação da alta administração, que ilustramos no quadro abaixo:

A Alta Administração NÃO:
...se responsabiliza pelas políticas de TI (51%)
...designou formalmente um Comitê de TI (48%)
...estabeleceu objetivos de desempenho de gestão e uso de TI (57%)
...definiu indicadores de desempenho de gestão e uso de TI (76%)

Fonte TCU – pesquisa de 2010

Como podemos constatar a partir dos resultados do quadro acima, ainda não existe um envolvimento estratégico da alta administração dos órgãos públicos, que equivocadamente, entende que o assunto deve ser de responsabilidade dos órgãos de TI. Os órgãos do governo federal têm orientado, constantemente, a alta administração dos órgãos públicos a participar com ações estratégicas para a definição dos objetivos institucionais de TI; da escolha de indicadores para cada objetivo; da criação de metas para cada indicador e, finalmente, de mecanismos para acompanhar desempenho da TI em sua instituição.

Desta forma pretende-se que a Tecnologia da Informação desempenhe seu relevante papel estratégico na instituição, agregando valores aos seus produtos e/ou serviços e auxiliando a promoção das inteligências competitivas e institucionais, à medida que seus recursos computacionais possibilitem a

geração de cenários decisórios produzidos com as informações oportunas e com os conhecimentos personalizados.

Concluímos este plano com o sentimento de que temos de envolver cada vez mais os altos gestores da UFF (reitor, pró-reitores e superintendentes) municiando-os com novos conhecimentos sobre a Governança de TI, para que a implementação das ações contidas neste PDTIC tenha sua participação nas decisões sobre a gestão de riscos, princípios, arquitetura, infraestrutura, necessidades de aplicação para o negócio, e investimentos e priorização.

17 – ANEXOS

ANEXO I - REALIZACOES PRINCIPAIS DA STI EM 2011.
ANEXO II - PROJETOS PDTIC.
ANEXO III – Topologia da RedeUFF.
ANEXO IV – Política de Segurança da Informação-v10.0.1.00.
ANEXO V – Norma de Utilização de Recursos Computacionais -v3.04.
ANEXO VI – Norma de Aquisição de Recursos computacionais v2.04.
ANEXO VII – Processos de Desenvolvimento de Sistemas_v1-2.
ANEXO VIII – Portaria STI.

ANEXO I - REALIZAÇÕES PRINCIPAIS DA STI EM 2011

No último ano, a STI atingiu alguns dos objetivos propostos inicialmente, dos quais vale à pena destacar como principais:

• Apoio à gestão superior da UFF para operacionalizar a reestruturação administrativa na UFF, com as devidas adaptações nos sistemas corporativos.

• Introdução da função de Governança de TI no início de 2011, como forma de dotar a STI de procedimentos para melhorar a comunicação com as diretrizes do governo federal.

• Revisão do Plano Diretor de Tecnologia da Informação (PDTIC), para o período de 2011-2014, com o conseqüente alinhamento ao PDI da UFF, à EGTI 2011- 2012 do SISP / SLTI / MPOG.

• Revisão da norma de acesso aos recursos computacionais na UFF e da Política de Segurança da Informação na UFF.

• Revisão das regras para aquisição de hardware e software (esta última passando a contar com a justificativa do docente sobre a necessidade da aquisição de hardware ou software para aplicação específica em pesquisa).

• Revisão da Metodologia de Desenvolvimento de Sistemas com a adoção de gestão através da implantação do Escritório de Projetos (onde toda a grande solução de TI passa a se tornar um projeto), mapeamento de processos e metodologia de desenvolvimento ágil.

• Elaboração de modelo de ACORDO DE NÍVEL DE SERVIÇO (ANS) para aplicação na renovação do contrato número 064/2010-PG, do registro da natureza do serviço e introdução de critérios de medição de desempenho.

• Manutenções corretivas no sistema "Relatório Anual de Docentes – RAD", com as melhorias de desempenho e segurança para departamentos e docentes, e implantação de novos relatórios para medição da produção departamental por tipos de produtos.

• Melhoria dos processos das consultas públicas, proporcionando um maior número de informações aos clientes.

• Planejamento, com os respectivos órgãos gestores, das necessidades de integração de sistemas (SIRH, SIORG, SIAD, SAPG e SAEP).

• Ações de apoio à gestão administrativa da UFF com o início do trabalho de integração dos sistemas de processos, patrimônio e de recursos humanos, ao Sistema de Controle do Organograma da UFF.

• Apoio ao processo de transferência de dados corporativos às bases de sistemas informatizados do governo federal, como PINGIFES (SESU), CADASTRO NACIONAL DE DOCENTES (INEP), a RELAÇÃO DE INGRESSANTES E CONCLUINTES PARA O ENADE (INEP), e SISTEMA DE COLETA DE DADOS DE PÓS-GRADUAÇÃO (CAPES).

• Lançamento da 6ª. versão do sistema de controle dos Laboratórios de Graduação do Projeto InfoLab.

• Ampliação da utilização da Sala de Videoconferência na STI.

• Modernização do serviço de Webmail.

• Lançamento do Portal WEBTV 2.0.

• Readequação do sistema de segurança central e da rede de serviços da RedeUFF.

• Readequação dos sistemas de e-mail e webmail, aumentando a performance, estabilidade, confiabilidade e inclusão de ferramentas para o usuário, com a implantação de sistemas anti-spam.

• Implementação do serviço de ligações DDD/DDI com a utilização do serviço gratuito VoIP da RNP e com canal digital da Embratel com tarifas diferenciadas para locais fora do alcance da RNP.

• Otimização da infraestrutura de consultoria para aquisição de equipamentos de informática, com qualificação da equipe e definição de normas e critérios.

• Aumento da utilização do UFFMAIL (para atendimento a demanda deste serviço para alunos de graduação).
• Modernização sistema CPPD, para viabilizar concursos para contratação de novos docentes.

• Central de atendimento na STI para melhorar nossa comunicação com o cliente e absorver, de forma centralizada, as demandas recebidas pela STI.

• Planejamento / implantação de novas metodologias de gestão, com a “projetização” das atividades, proporcionando o melhor acompanhamento dos resultados.

• Início da implantação da Sala Segura para suporte à implantação do sistema AGHU.

• Início de trabalhos para homologação de um padrão wi-fi na UFF.

• Criação de controle inicial para registro dos treinamentos realizados por servidores da STI (informando o nome do treinamento e quantos servidores foram treinados).

EMENTA: Propõe os termos da Política de Segurança da Informação da Universidade Federal Fluminense.

A Política de Segurança da Informação da Universidade Federal Fluminense tem seus termos propostos, conforme segue:

Art.1. As questões relativas à Segurança da Informação, bem como, a administração e gestão da Segurança da Informação em Ambiente Computacional da Universidade Federal Fluminense ficarão única e exclusivamente a cargo da Área de Segurança da Informação da Superintendência de Tecnologia da Informação – STI da UFF.

Art.2. A Área de Segurança da Informação da STI será a responsável pela edição de Políticas, Normas e Procedimentos Institucionais que se façam necessárias para a garantia da Segurança e mitigação de riscos ao ambiente de Tecnologia da Informação – TI da UFF.

Art.3. A aprovação e promulgação de Normas e Procedimentos de Segurança da Informação Institucionais ficarão a cargo do Comitê de Tecnologia da Informação (COTI), enquanto para Políticas ficarão a cargo do Gabinete Reitor da UFF.

Art.4. Esta Política se aplica a todos os colaboradores da Universidade Federal Fluminense e seus órgãos, nos diversos níveis hierárquicos e vínculos – servidores, estagiários, trainees, temporários, fornecedores, clientes, terceirizados, etc – que a qualquer momento tenham necessidade de utilizarem os recursos de TI.

Art.5. Esta Política deverá obrigatoriamente sofrer revisões, no mínimo uma vez a cada ano-calendário, visando à garantia de manutenção da mesma atualizada, e condizente com as melhores práticas de Segurança, as novas ameaças, a evolução tecnológica da UFF, o crescimento da Instituição e suas constantes mudanças.

Art.6. A Área de Segurança da STI, juntamente com os Órgãos de Recursos Humanos, Jurídico da UFF e o Comitê de Tecnologia da Informação, deverá definir uma matriz de responsabilidades referente às aprovações e aos aprovadores no âmbito de TI, devendo, esse documento ser revisado no mínimo uma vez em cada ano-calendário. Essa matriz deverá obrigatoriamente contemplar os variados tipos e eventos de liberações de acesso e os respectivos responsáveis pela aprovação dos mesmos. Os usuários responsáveis deverão ser comunicados e estarem cientes que além da aprovação, poderão ser diretamente ou possuem corresponsabilidade acerca de eventos de mal-uso, descumprimento de normas ou ainda, infrações legais originadas de autorizações oferecidas pelos mesmos.

Art.7. Os processos, políticas, normas e procedimentos de Gestão de Riscos em Segurança da Informação deverão ser definidos pela Área de Segurança da Informação da STI e revisados periodicamente, no mínimo uma vez a cada ano-calendário.

Art.8. A Área de Segurança da Informação da STI será responsável pela edição e aplicação dos planos de Gerenciamento e Reposta a Incidentes, devendo os mesmos ser suportados por Política, Norma ou Procedimento específicos para tal, bem como, chancelados pelo Comitê de Tecnologia da Informação.

Capítulo I
Das Definições

Art.9. Para efeito dessa política considere-se:

I) **Ambiente Computacional:** é o conjunto de recursos computacionais separado para uma determinada função. Subdivido em:

I.I) **Produção:** ambiente que possui os dados reais do sistema, aquele que os usuários utilizam para as funções diárias e que cujas informações possuem valores legais e são aproveitadas pela instituição. Por possuir dados reais, é considerado ambiente extremamente crítico para a Segurança das Informações da Instituição e por isso, seu acesso deve ser limitado e somente liberado a quem realmente possui necessidade de utilizá-lo em tarefas do dia-a-dia e de alimentação de informações para o sistema.

I.II) **Homologação:** ambiente no qual são feitos os testes de um sistema e que um grupo restrito de usuários tem acesso para validação de funções de um novo sistema ou de novas funções para um sistema pré-existente. Possui cópias desatualizadas dos dados de produção. Por possuir dados reais, mesmo que desatualizados, possui razoável criticidade quando ao comprometimento da Segurança das Informações Institucionais.

I.III) **Desenvolvimento:** é o ambiente no qual os desenvolvedores de sistema possuem acesso para criar um novo sistema ou novas funções para um sistema pré-existente. Obrigatoriamente possui esquemas reais (tabelas, campos em tabelas) porém, preenchidos com dados falsos. Não compromete a Segurança das Informações da Instituição.

II) **Perfil de acesso:** conjunto de regras de computação que liberam apenas determinadas operações em um sistema. É o perfil de acesso que determina as permissões de um usuário, ou seja, o que ele pode ou não fazer em um sistema.

III) **Usuário Normativo:** usuário de área, ou seja, não é necessariamente um Analista de TI, que possui conhecimento profundo da área operacional e recebe conhecimento acerca dos perfis de usuário de um determinado sistema. É ele o responsável por aprovar a liberação de acesso de um determinado perfil de acesso a um determinado usuário. Ou seja, é ele o responsável por afirmar que as funções de um determinado usuário são compatíveis com o perfil a ser liberado para o mesmo.

IV) **Área Normativa:** área da Instituição que é responsável pelas informações contidas em um sistema. O usuário normativo deve obrigatoriamente pertencer à Área Normativa.

Art.10. Compõem os recursos computacionais da UFF equipamentos integrantes de quaisquer ambientes computacionais supracitados, sejam estes de quaisquer tipos ou com quaisquer finalidades (computadores, notebooks, telefones, switches, hubs, impressoras, periféricos, etc.), independente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta Política.

Capitulo II
Das Diretrizes Gerais

Art.11. A Segurança da Informação deve ser responsabilidade de todos, não apenas da área de TI. Desta forma, deve refletir em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos, etc.

Art.12. A Superintendência de Tecnologia da Informação irá providenciar os recursos humanos e materiais necessários para implementação das diretrizes estabelecidas nesta Política, bem como orientar todos os usuários quanto as suas ações que serão tomadas, além de divulgar os preceitos de segurança da informação a serem observados por todos, inclusive, nas divisões, órgãos e campi da UFF que possuem ambiente de TI distinto, com maior ou menor integração com o restante da instituição;

Art.13. A utilização de informação e dos recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art.14. A utilização de recursos (sistemas, correio eletrônico, espaço em disco, equipamentos, etc.) disponibilizados pela instituição ou integrados ao ambiente desta (rede e afins), deve ser feita segundo os padrões e procedimentos definidos pela STI, visando manter a disponibilidade e o desempenho das aplicações.

Art.15. A conexão de equipamentos de terceiros na rede da instituição somente será permitida se não apresentarem risco ao ambiente corporativo e estiverem de acordo as políticas da instituição aplicáveis aos demais equipamentos, bem como, houver sido analisada e declarada adequada pela STI.

Art.16. As informações classificadas como confidencial e/ou reservada requerem alto grau de controle e proteção contra acessos não autorizados, como também, aquelas que necessitem de sigilo por força de lei ou contrato são candidatas naturais à obtenção dessa classificação. O direito de acesso a estas informações requer autorização expressa do Usuário Normativo e é regida por política específica de Classificação da Informação.

Art.17. A utilização indevida dos recursos computacionais pode provocar sanções a serem definidas pela STI e a Área de Segurança da Informação da STI, dentre elas a suspensão dos acessos, e deve ser notificada à Área de Segurança da Informação.

Art.18. Qualquer violação dessa política constitui base para uma medida disciplinar, inclusive o término do contrato empregatício, conforme Política Disciplinar, bem como, às sanções previstas por lei.

Capitulo III
Da Classificação das Informações

Art.19. A Classificação das Informações na UFF será regulamentada por política específica acompanhada de procedimentos específicos de manipulação, salvaguarda, transporte, criação e edição.
1.Toda informação criada no ambiente da UFF não classificada explicitamente será considerada informação Reservada

Capítulo IV
Da gestão da Segurança das Informações e suas responsabilidades

Art.20. A responsabilidade pela gestão da Segurança da Informação é atribuída aos agentes envolvidos no processo de criação, salvaguarda, transporte e destruição da informação, sendo assim caracterizados:

Normativos: responsáveis pela classificação da informação, pela definição de perfil do usuário e o tipo de acesso às informações;

Usuários: todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação dessa política;

Custodiante: responsável pela guarda da informação com segurança. Na UFF e nos seus campi, esse agente é a Área de Segurança da Informação da STI, que terá a incumbência de implementar e controlar as autorizações de acesso à rede, correio/e-mail, internet, sistemas, servidores, etc.; monitorar o uso adequado dos recursos liberados, bem como, de implementar e operacionalizar os mecanismos de segurança da informação.

Art.21. Os usuários normativos de natureza específica serão designados pelos 1º nível de reporte das áreas usuárias.

Art.22. Os gestores das Unidades Organizacionais da UFF são Usuários Normativos das informações pertencentes ao domínio de sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas. Para tanto, devem formalizar estas delegações junto à Área de Segurança da Informação da STI.

Capitulo V
Da Segurança Física do Ambiente de TI

Art.23. Todos os equipamentos, incluindo suas movimentações, que compõem a estrutura do ambiente computacional da UFF, tais como servidores, roteadores, switches, hubs, controladores, impressoras, meios óticos e magnéticos de backup, computadores, etc., devem ser devidamente autorizados e registrados pela Divisão de Atendimento Técnico da STI.

Art.24. A UFF manterá dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, etc.) e lógica (vírus, acesso não autorizado, invasões, etc.) compatíveis com os requisitos definidos nessa política. Cabe à STI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos. Nenhum fluxo de informações poderá existir sem que passe pelas camadas de proteção lógica.

Art.25. Para os sistemas classificados como de missão crítica, será utilizado hardware que disponha de recursos de redundância de processador, disco, energia, etc., bem como, equipamentos de prevenção e combate a incêndios (SPCI), além de controle da corrente elétrica (rede estabilizada), temperatura e umidade e acesso físico e lógico restrito.

Capitulo VI
Da Segurança Lógica do Ambiente de TI

Art.26. Cabe à Área de Segurança da Informação da STI garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estando em conformidade com as diretrizes descritas nessa Política, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela área de segurança.

Art.27. Todo programa ou transação desenvolvido ou adquirido para execução no ambiente UFF deve, obrigatoriamente, conter as verificações de autorização de execução em perfeita sintonia com o ambiente tecnológico em que será processado. Não haverá exceção à verificação de autorização para execução de qualquer programa ou transação. A princípio, tudo que não for explicitamente permitido, está negado.

Art.28. Todo novo programa ou transação adquirido para execução no ambiente UFF deverá ser submetido à análise da Área de Segurança da STI afim de verificar sua conformidade.

Art.29. Nenhuma senha pessoal será gravada no código-fonte de programas, tampouco em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica da STI para desenvolvimento e/ou aquisição de sistemas, softwares e afins.

Art.30. O acesso – mesmo que de simples consulta – aos arquivos ou tabelas de senha não será permitido, em nenhuma circunstância, a nenhum colaborador. Tal restrição será provida por mecanismos de segurança lógica ou criptografia;

Art.31. Toda conta de acesso sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela Área de Segurança da STI, sem prévia autorização do proprietário ou da Gerência para isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados. A exceção dessa regra é para usuários com primeiro nível de reporte à Reitoria, que serão contatados antes do recurso ser desabilitado;

Art.32. É proibida a desinstalação, nas estações usuárias, de softwares ou hardwares, que são utilizadas para realizar controle físico e lógico dos recursos disponíveis. Caso isso ocorra por procedimento indevido, o fato será comunicado, imediatamente, ao Superior Imediato e à Divisão de Atendimento Técnico, que apurará as causas, corrigirá o problema e providenciará a reinstalação;

Art.33. Somente será permitido o uso de recursos homologados e autorizados pela Instituição, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor. A utilização destes sem licenças correspondentes é crime, previsto na Lei 9.609, de 19 de Fevereiro de 1998. Portanto, qualquer usuário que exponha a Instituição a sansões jurídicas por utilização de softwares não homologados, independente de sua classificação (shareware, freeware, demo, etc.) sem respaldo das respectivas licenças, está sujeito às medidas disciplinares previstas, bem como, às sanções previstas por lei;

Art.34. A Homologação de recursos computacionais será de única e exclusiva responsabilidade da STI, sendo regida por norma e procedimento específico de Homologação de Software e Homologação de Hardware.

Art.35. Nenhum software, independente de suas condições comerciais, será instalado ou baixado para equipamentos UFF pelo próprio usuário, cabendo esta tarefa exclusivamente aos usuários alocados nas gerências e divisões da STI, que tem essa atividade inclusa no seu papel funcional. A exceção a essa regra somente poderá ocorrer mediante aprovação expressa da área de Segurança da STI, respeitando-se as premissas do item 4 dessa política. Tais liberações terão sempre efeito pontual e nunca serão vistas como permanentes e genéricas.

Art.36. A STI irá restringir as pessoas que poderão ser administradoras das respectivas estações de trabalho.

Art.37. No caso de contas de acesso standard e impossíveis de serem eliminadas ou alteradas, as senhas standard (que vem junto com o produto) serão, obrigatoriamente, modificadas imediatamente após a disponibilização do sistema e/ou ambiente, sem que haja solicitação específica sobre isso.
Art.38. É obrigatória e existência de planos de segurança e de infraestrutura para implantação de sistemas de informação, sendo que não serão implementados se trouxerem fragilidades que comprometam a segurança do ambiente UFF.

Capitulo VII
Do uso e formação das senhas

Art.39. Uma senha segura possui ao menos oito caracteres, inclui uma combinação de letras, números e símbolos e é fácil de ser lembrada, mas difícil de ser “quebrada”. Para a formação das senhas, serão adotados os seguintes critérios:

I) Tamanho mínimo de 8 caracteres.
II) Nunca podem ser nulas ou estar em branco.
III) Nunca visíveis na tela onde são informadas para atualização ou login.
IV) Nunca podem começar com os 3 caracteres iniciais do ID.
V) Mínimo de 2 dígitos numéricos.
VI) Mínimo de 2 caracteres alfanuméricos.
VII) Impedir a repetição de um mesmo caractere 3 vezes seguidamente.
VIII) Vetar a reutilização de ultimas 5 senhas utilizadas.
IX) Serem bloqueadas após 5 tentativas consecutivas e mal sucedidas de acesso.
X) Passar por rotinas de crítica que impeçam a utilização de senhas “fracas” ou “facilmente quebráveis”

XI) Evitar palavras dicionarizadas.

Art.40. Todas as senhas expirarão independentemente da vontade dos usuários, no máximo, a cada 45 dias. Além disso, todas as senhas iniciais – definidas pela Área de Segurança da Informação da STI quando da liberação do acesso – serão expiradas e, ao primeiro acesso de cada usuário, forçada a sua troca.

Art.41. As senhas pessoais podem ser trocadas pelo próprio usuário, independentemente da sua data de expiração. Porém, deverão ser impossibilitadas de serem trocadas mais de 1 vez no mesmo dia.

Art.42. Nenhum colaborador poderá usar de sua ascendência hierárquica ou funcional sobre outrem para determinar ou obrigar que este compartilhe sua senha pessoal de acesso com quem quer que seja. O usuário que porventura receba esse tipo de solicitação deve comunicar o fato à Área de Segurança da Informação da STI.

Art.43. O compartilhamento de senhas, individuais é proibido para todos os níveis da instituição. Da mesma forma, abrir uma conexão autenticada para deixar que outra pessoa a utilize. Em hipótese alguma, um usuário poderá passar sua senha pessoal de acesso para outrem. Tal ação, uma vez detectada, terá classificação de gravidade em função do ambiente em que ocorreu e será devidamente reportada aos superiores hierárquicos dos usuários e ao DDRH.

Art.44. Qualquer tentativa de “quebrar” (tentar descobrir) a senha pessoal de acesso de outra pessoal, ou mesmo invadir ambientes ou sistemas sujo acesso lhe é negado, serão notificadas aos superiores hierárquicos, e poderá resultar em medidas disciplinares apropriadas, conforme disposto na **Política Disciplinar**.

Art.45. É dever de todos, zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando ser descoberta facilmente por outra pessoa.

Capitulo VIII
Da Segurança de Acessos

Art.46. A conta de acesso e a **senha** de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representem nível de delegação concedida para o desempenho de suas funções.

Art.47. Os acessos externos a recursos da instituição (acesso remoto de colaboradores, terceiros, fornecedores, clientes, e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia, segundo instruções detalhadas caso a caso e realizadas por intermédio de soluções técnicas institucionais.

Art.48. O acesso à internet é permitido por intermédio de sistema de segurança institucionais. É proibido o acesso direto à internet por intermédio de provedores externos estando conectado à rede UFF.

Art.49. Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processo de automação e/ou informação somente deverão ocorrer utilizando soluções corporativas definidas pelo STI, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

Capitulo IX
Do Controle de Acesso

Art.50. A Área de Segurança da Informação da STI deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso incompatíveis com a sua função, ou seja, cada usuário terá uma única conta de acesso por aplicação.

Art.51. A Área de Segurança da Informação definirá e adotará um padrão de identificação de usuários que permitirá associar, de maneira única, cada direito de acesso à pessoa que o detém e concederá direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados. Tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

Art.52. No caso de fiscais de outros órgãos públicos, mesmo não existindo vínculo direto, as pessoas também poderão ser cadastradas nos sistemas de RH, associados a um colaborador responsável e também controlados por data de vigência lógica.

Capitulo X
Da Segregação de Ambientes e Funções

Art.53. A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes as diretrizes a seguir:

I) Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais.

II) Os ambientes que não sejam de produção – ou seja, de teste, de homologação, de desenvolvimento e outros – devem ser de acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas. Estes usuários, nos ambientes de produção, podem efetuar, no máximo, operações de consulta.

III) O acesso às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas de informação, estando completamente vetado qualquer tipo de acesso direto. Os casos extremos de necessidade de liberação serão aprovados pela Área de Segurança da STI em conjunto com o usuário com nível gerencial da área solicitante.

IV) Todo objeto, tais como programas, telas, funções, etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes o arquivo fonte original.

V) Deve existir nos ambientes de produção, sempre que tecnologicamente possível, um controle automático das versões dos programas-fonte. Este controle possibilitará a recuperação de versões recentes (dentro dos 6 meses predecessores e das 6 ultimas versões), assim como a identificação do responsável pela sua implantação. O acesso aos programas-fonte, principalmente de inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acesso específicos e registrado em trilhas de auditoria.

Capitulo XI
Do Plano de Contingência

Art.54. Para enfrentar situações de interrupção dos sistemas de informação, com consequente paralisação das atividades da UFF, a STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de operação.

Art.55. O Plano de Contingência deverá passar por revisões periódicas, no mínimo uma vez a cada ano-calendário.

Art.56. O Plano de Contingência deverá ser exercitado no mínimo 2 vezes ao ano.

Capitulo XII
Da Propriedade Intelectual

Art.57. Todos os sistemas, projetos e/ou configurações desenvolvidos para atender as necessidades e aos interesses da Instituição são de propriedade única e exclusiva da UFF, e somente poderão ser cedidos, comercializados ou distribuídos mediante a aprovação do STI. Essa regra deve ser formalizada em todos os contratos com fornecedores e prestadores de serviço ou atividades de desenvolvimento realizadas pela equipe de desenvolvimento UFF.

Art.58. A documentação dos sistemas de informação e projetos desenvolvidos, devem ser disponibilizadas em meio ótico ou magnético, contendo:

I) Códigos fonte dos objetos (programas, telas, transações, etc.) desenvolvidos;

II) Manual do Usuário e/ou Help On-Line, desde que apresente explicações sobre funcionalidades e não apenas preenchimento de campos;

III) Diagrama de Contexto e Especificação Funcional;
IV) Diagrama de Casos de Uso e Casos de Uso;
V) Dicionário de Dados (DD);

VI) Diagrama de Fluxo de Dados (DFD) ou Modelo de Transição de Dados (em projetos de automação, é indispensável os dois);

VII) Modelo de Entidade-Relacionamento (MER) ou Modelo de Objetos;

VIII) Diagrama de Classes

IX) E quaisquer outros artefatos de projeto e desenvolvimento gerados pela metodologia de projeto e desenvolvimento empregada no projeto.

Art.59. No caso dos sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros, a STI exigirá em contrato a disponibilização e atualização da documentação pertinente. Os pagamentos a serem efetuados ao fornecedor estarão condicionados à entrega de tal documentação, que poderá ser proporcional aos produtos entregues em cada fase do projeto.

Capitulo XIII
Da Auditoria e das Trilhas de Auditoria

Art.60. A Auditoria poderá ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informação). Havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, podendo a Auditoria auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art.61. A STI deve providenciar os recursos tecnológicos para que as trilhas de auditoria sempre existam e fiquem disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os arquivos conhecidos como trilhas de auditoria.

Art.62. As trilhas de auditoria de um determinado sistema devem ser centralizadas evitando a sua dispersão em vários arquivos e ser de fácil acesso a quem de direito.

Art.63. As trilhas de auditoria devem registrar automaticamente todas as operações críticas efetuadas, e serão constituídas de, pelo menos, os seguintes campos: identificador do usuário (nominal, não podendo ser somente IP ou MAC Address), data da operação, horário da operação, operação realizada, dados antes da operação e dados após a operação.

Art.64. Sempre que surgir um novo ambiente lógico na instituição, a STI tomará a iniciativa de reunir-se com os Usuários Normativos correspondentes para deliberar sobre a criação das trilhas de auditoria.

Art.65. As trilhas de auditoria devem estar disponíveis para consulta por um prazo mínimo de 1 (um) ano, além de protegias contra inclusão, exclusão ou alteração de dados. As únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capitulo IVX
Referências Normativas

Art.66. Este documento se ampara e referencia pelos instrumentos normativos apresentados conforme segue:

I) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Publica Federal.
II) Decreto 4.553 de 27 de dezembro de 2002 – Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Publica Federal, e dá outras providências.
III) Lei 9.609 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.
IV) Instrução Normativa GSI/PR nº 01 de 01 de julho de 2008 – Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
V) Norma Complementar nº 03 de junho de 2009 à Instrução Normativa GSI/PR nº01 – Recomenda diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.
VI) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008.
VII) Portaria SLTI/MP nº05 de 14 de julho de 2005 – Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.
VIII) ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação.
ABNT NBR ISO/IEC 27002:2005 – Código de Praticas para Gestão de Segurança da Informação.

EMENTA: Propõe os termos da Norma deUtilização de Recursos Computacionais da Universidade Federal Fluminense.

A **Norma de Utilização de Recursos Computacionais da Universidade Federal Fluminense** tem seus termos propostos conforme segue:

Art. 1 - Essa Norma se aplica a todos os colaboradores de todas as unidades da UFF, alunos, estagiários, trainees, temporários, substitutos, fornecedores e terceirizados vinculados à UFF, que a qualquer momento tenham acesso a recursos da TI.

Art. 2 - A Superintendência de Informática utilizará recursos tecnológicos para detecção, bloqueio e remoção de utilizações indevidas. Caso seja identificado algum uso impróprio dos recursos de informática, o usuário terá suspensão imediata dos recursos disponibilizados e notificados seus superiores hierárquicos, bem como, esta sujeito a demais sanções aplicáveis de acordo com seu vínculo dom a Instituição.

Art. 3 - Os recursos computacionais são bens da Instituição e são disponibilizados como ferramentas para permitir que os usuários desempenhem suas tarefas e para uso predominantemente das atividades profissionais ou acadêmicas, devendo em ambas atividades serem respeitados os Instrumentos Normativos institucionais.

Art. 4 - Nenhum software que não cumpra as políticas da Instituição ou os acordos de licenciamento e direitos autorais aplicáveis a cada situação pode ser adicionado ao sistema de comunicação eletrônica da UFF. Não se admite também a transmissão de arquivos, imagens ou jogos interativos que violem estas premissas.

Art. 5 - Qualquer software, mesmo que licenciado pelas licenças publicas ou opensource devem estar aderentes às políticas da Instituição, bem como, terem sido homologados/aprovados pelo STI.

Art. 6 - A Instituição reserva-se o direito de controlar, monitorar e até mesmo bloquear a utilização de sistemas de informática, o acesso à Internet de todos os equipamentos interligados ao sistema de TI e de acessar mensagens e arquivos eletrônicos gerados pelos usuários, a seu critério e a qualquer momento. Assim, o monitoramento, tanto do ambiente quando do seu conteúdo, pode acontecer para evitar transtornos decorrentes do uso indevido para fins ilegais, fraudulentos ou que prejudiquem a terceiros, sem que isso implique em violação dos incisos X e XII do artigo 5º da CF/1988

Capítulo I
Das Definições

Art. 7 - Para efeito dessa norma considere-se:

I) Recurso Computacional: São entendidos como computadores, notebooks, elementos de rede, cabeamento, sistemas e softwares, appliances e demais dispositivos integrantes da RedeUFF ou nela conectados.

II) Nível de Reporte: São os níveis hierárquicos, contados a partir do maior (Reitor) em ordem decrescente. Trata-se de um padrão muito utilizado para definição de níveis hierárquicos evitando-se tratar os mesmos por cargos, que podem possuir as mesmas prerrogativas e responsabilidades tendo títulos diferentes. O maior nível de reporte é o Zero, que no caso da UFF trata-se do Magnifico Reitor. Os servidores imediatamente subordinados ao reitor são considerados Primeiro Nível de Reporte (são exemplos: Pró-Reitores e Superintendentes). Enquanto os servidores imediatamente subordinados ao Primeiro Nível de Reporte são considerados Segundo Nível de Reporte e assim, sucessivamente.

III) Homologação: Processo definido formalmente, no qual a STI e suas áreas especialistas efetuam testes e definem que um determinado recurso pode ser utilizado no ambiente de TI da UFF, atestando Segurança, Confiabilidade, ausência de incompatibilidade, adequação à estrutura existente e demais requisitos de adequação.

Capitulo II
Das Responsabilidades

Art. 8 - Para efeito dessa Norma, as responsabilidades dos usuários quanto a aprovações faz-se conforme a seguir:

Art. 9 - Em todas aprovações abaixo a Área de Segurança da STI terá função consultiva obrigatória,
devendo ser consultada nos processos e ainda podendo em casos externos vetar aprovações.

Art. 10 - Primeiro nível de reporte à reitoria

I) Aprovar a concessão de direitos de acesso remoto aos sistemas da UFF para colaboradores sem nível formal de reporte.

II) Aprovar as solicitações para criação de mais de um login por aplicação para mais de usuário.

III) Liberar recursos através de conta de acesso individualizada e temporária (não superior a 15 dias) e, com recursos que não envolvam atualização de dados em sistemas aplicativos para prestadores de serviços de consultoria e auditoria, de caráter não repetitivo, caracterizado por serem de curta duração.

Art. 11 - Primeiro nível de reporte à reitoria em conjunto com a Superintendência de Tecnologia da Informação – STI e a Área de Segurança da STI

I) Aprovar as solicitações de acesso e a conexão de equipamentos de informática de terceiros na rede UFF para prestadores de serviço.

II) Aprovar as solicitações de direitos de acesso para colaboradores UFF, se estas ainda não estiverem integradas ao ambiente de TI da UFF.

Art. 12 - Primeiro nível de reporte da área envolvida

I) Aprovar liberação, temporária, de recursos computacionais lógicos individualizados de usuários ativos, licenciados e ex-colaboradores para outras pessoas da ativa.

II) Aprovar aquisição e acesso a dispositivos de mídia removível.

Art. 13 - Usuário com nível de reporte superior ao do usuário solicitante

I) Aprovar solicitações de cadastramento, alteração, bloqueio, exclusão de usuários e solicitar à Área de Segurança da Informação do STI relatório analítico de acessos à Internet.

Art. 14 - Segundo nível de reporte do usuário normativo

I) Aprovar a criação de contas de acesso genérico somente para consulta, em casos de aplicação configurada para uso público (garantido através de um perfil de acesso especialmente construído para esse fim).

Art. 15 - Segundo nível de reporte do usuário

I) Aprovar a liberação de recursos computacionais em ambientes de produção para estagiários.

Art. 16 - Usuário normativo

I) Fazer revisões de acesso aos recursos do qual é normativo, podendo solicitar remoção e/ou readequações de perfis/permissionamentos para as pessoas já com acesso sem necessidade de aprovação gerencial.

II) É obrigatório que os normativos façam revisões periódicas de acesso, aos recursos sob suas responsabilidades, pelo menos uma vez ao ano-calendário e dependendo da criticidade ou confidencialidade do recurso recomenda-se a adoção de periodicidade menor. Para essa atividade poderão solicitar levantamentos à Área de Segurança da STI sem necessidade de aprovação gerencial.

III) Para ambientes de criticidade ou confidencialidade elevadas, a Área de Segurança da Informação da STI em conjunto com o respectivo usuário normativo do ambiente definirão periodicidade inferior a uma vez ao ano-calendário.

Capítulo III
Das Diretrizes Gerais

Art. 17 - Os equipamentos de computação, programas, dados e informações armazenadas nos sistemas informatizados deverão ser adequadamente protegidos contra danos, perda, roubo, duplicação, alteração ou acesso não autorizado.

Art. 18 - Somente será concedido acesso a sistemas ou softwares licenciados/comerciais se houver limite de licenças disponíveis na instituição, caso contrário, será providenciado formalmente o acréscimo das mesmas ou então processada substituição da licença por alguém que seja autorizado.

Art. 19 - Havendo solicitação a algum recurso considerado crítico para a Instituição ou conflitante com as atribuições que o usuário possuir, a solicitação somente será atendida após análise e parecer do 1º nível de reporte ao qual o usuário é subordinado por meio de comunicação realizada pela Área de Segurança da Informação informando os riscos envolvidos.

Art. 20 - Não é permitida a utilização de equipamentos de hardware, exceto notebooks e ainda esses com devidas restrições, de propriedade do próprio usuário.

Art. 21 - O Artigo 4 do Capitulo III desta Norma também aplica-se a quaisquer tipos de softwares que não sejam homologados pela STI.

Capítulo IV
Da Classificação dos Recursos Computacionais

Art. 22 - Para efeito dessa norma os recursos computacionais são classificados pela Área de Segurança da Informação da STI conforme a seguir:

I) Recursos Comuns: rede, diretórios compartilhados específicos da unidade, correio eletrônico (e-mail), aplicações classificadas como de uso público

II) Recursos Específicos: sistemas de informação, sistemas gerenciadores de bancos de dados (SGDB's), sistemas de automação, etc.

Capítulo V
Do Direito de Uso dos Recursos Computacionais

Art. 23 - Possuem direito de uso dos recursos computacionais, usuários – servidores efetivos da Instituição, Estagiários, Temporários, Substitutos e Terceiros Vinculados à UFF, em situação regular junto à UFF e seu Órgão de Recursos Humanos, mediante autorização prévia e por tempo determinado.

Art. 24 - O direito de uso de qualquer recurso computacional cessa quando o usuário terminar o seu vínculo regular com a Instituição ou tiver o mesmo suspenso.

Capitulo IV
Das Responsabilidades Individuais

Art. 25 - É responsabilidade de cada usuário o conhecimento e práticas das regras e procedimentos definidos nessa política durante o uso dos recursos computacionais da Instituição.

Art. 26 - Não devem ser transmitidas/armazenas informações que caracterizem propaganda política, ameaças, difamações, ofensas ou que induzam a qualquer forma de discriminação ou bulling.

Art. 27 - Garantir o sigilo de suas senhas de acesso aos ambientes lógicos e aos computadores da Instituição. A senha é pessoal e intransferível, devendo, portanto, ser trocada periodicamente e conter códigos de difícil decodificação. Da mesma forma, não ceder sua senha ou utilizar a senha de outros usuários.

Art. 28 - Antes de ausentar-se de seu local de trabalho, o usuário deverá fechar todos os programas acessados e/ou bloquear o computador através de senha, utilizando o recurso de proteção do sistema operacional utilizado no computador, evitando, dessa maneira, o acesso por pessoas não autorizadas.

Art. 29 - Não fazer uso de senhas, códigos e contas de acesso de colegas de trabalho, de superiores ou terceirizados sob qualquer pretexto.

Art. 30 - Não fazer uso de senhas com menos de 8 caracteres ou triviais, tais como: nome do ambiente, caracteres repetidos, nome ou sobrenome do usuário ou de parentes, datas comemorativas ou qualquer outra sequencia de caracteres que seja de fácil identificação.

Art. 31 - Seguir sempre os critérios de formação de senhas definidos no Capítulo VII da Política de Segurança da Informação, ainda que o ambiente computacional legado não exija automaticamente tais processos.

Art. 32 - Zelar pela integridade física dos equipamentos de informática que utiliza ou tem sob sua guarda, não sendo permitida qualquer remoção, desconexão de partes, substituição ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes do ambiente de processamento de dados da Instituição.

Art. 33 - Respeitar a propriedade intelectual, não copiando, modificando, usando ou divulgando todo ou em parte texto, artigos, programas ou qualquer outro material, sem permissão expressa por escrito, do detentor dos direitos da mesma.

Art. 34 - Responsabilizar-se por qualquer operação (consulta, inclusão, exclusão ou alteração) efetuada nos ambientes lógicos, acessados de sua conta de acesso individual.

Art. 35 - Utilizar sempre programas antivírus atualizados e disponibilizados pela Instituição antes de acessar informações em disquetes, pen-drives, discos rígidos, CD’s ou DVD’s e quaisquer arquivos oriundos de fora da Instituição (via internet ou e-mail, por exemplo).

Art. 36 - Utilizar somente programas de computador que possuam as suas respectivas licenças de uso e que sejam autorizados (homologados) pela STI.

Art. 37 - Submeter à homologação da STI qualquer sistema de informação, desenvolvido ou adquirido, juntamente com sua respectiva documentação antes da entrada do mesmo em Ambiente de Produção.

Art. 38 - Não executar programas que tenham como finalidade a decodificação de senhas, a leitura de dados de terceiros, a exploração maliciosa de eventuais falhas tecnológicas, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços.

Art. 39 - Não executar programas, instalar equipamentos ou executar ações que possam facilitar o acesso à rede por pessoas não autorizadas.

Art. 40 - Respeitar áreas de acesso restrito, não executando tentativas de acesso às áreas ou maquinas alheias a suas permissões de acesso.

Art. 41 - Não fazer uso de direitos especiais de acesso ou de qualquer outro privilégio já extinto com o término do período de ocupação de cargo ou função dentro da Instituição.

Art. 42 - Não fazer uso de falhas tecnológicas possivelmente existentes no ambiente para obter acesso indevido a informações. Caso tenha conhecimento da existência de alguma falha, é dever reportar ao seu superior imediato ou diretamente ao responsável pelo ambiente afetado, juntamente com a Área de Segurança da STI.

Capítulo VII
Da Solicitação de Recursos Computacionais

Art. 43 - Cabe a cada gestor definir os recursos computacionais necessários para cada usuário e enviar a solicitação previamente aprovada à Área de Segurança da Informação da STI.

Art. 44 - Cabe a cada gestor também, se responsabilizar solidariamente por qualquer má utilização advinda de recursos por ele aprovados.

Art. 45 - As solicitações de utilização de recursos computacionais somente serão atendidas após verificação da situação do usuário nos sistemas de RH e Contratos/Terceiros. Somente obterão acessos colaboradores ativos e terceiros cujos contratos estejam vigentes e que realmente necessitem desses recursos para cumprimento de suas atribuições.

Art. 46 - Os usuários que não se enquadrem nestas situações ou possuam data de validade vencida ou em branco terão os direitos de acesso bloqueados de imediato, mesmo que ocorram solicitações a respeito. Se porventura existir mais de uma data de validade, prevalecerá sempre a validade mais curta.

Art. 47 - Somente serão processadas solicitações de cadastramento, alteração, bloqueio e exclusão de usuários que contenham justificativas explícitas por escrito (via e-mail ou aplicação específica) e aprovados por um funcionário com nível gerencial e reporte superior ao do usuário. Os colaboradores classificados como 3º nível de reporte e acima, poderão solicitar/aprovar as solicitações de recursos para si próprios, porém com justificativa, desde que sejam compatíveis com sua área de atuação.

Art. 48 - Todas as solicitações conterão explicitamente os recursos desejados, ficando vetado o atendimento a solicitações do tipo “liberar para X os mesmos acessos de Y”, a menos que seja específico para um único ambiente operacional. As solicitações que porventura surgirem dessa forma serão detalhadas pela Área de Segurança da Informação do STI e confirmadas pelo Gerente da área solicitante.

Art. 49 - Todas as solicitações serão arquivadas por um período mínimo de 5 anos.

Capítulo VIII
Da Solicitação de Recursos Computacionais para Estagiários

Art. 50 - Poderão ser liberados para estagiários somente recursos considerados como comuns.

Art. 51 - Os recursos liberados deverão ser em ambiente não produtivo (homologação, teste, etc.).

Art. 52 - Não são liberados acessos às informações classificadas como confidenciais ou quaisquer recursos computacionais específicos, tais como: baixa de software, acesso remoto, etc.

Art. 53 - Caso haja necessidade de atualizar informações específicas em sistemas institucionais (em produção) por exigência da atividade exercida, caberá ao 2º reporte da área do estagiário em conjunto com o usuário normativo do ambiente a decisão de liberação ao ambiente de produção.

Capítulo IX
Da Solicitação de Recursos Computacionais para Terceirizados

Art. 54 - A liberação de recursos para terceiros poderá ser feita para qualquer ambiente ou sistema necessário ao desempenho das atividades para as quais foi contratado. No entanto, deve ser evitado o compartilhamento de arquivos, recursos, ambientes, transações que possam provocar a exposição inadequada e manipulação indevida de informações reservadas ou confidenciais da Instituição.

Art. 55 - Áreas de armazenamento de arquivos não poderão ser liberadas para usuários terceirizados, exceto diretórios restritos criados especialmente para esse fim e que não poderão conter informações reservadas ou confidenciais.

Art. 56 - É responsabilidade da Contraparte UFF do contrato comunicar à Área de Segurança do STI quando ocorrer desligamento, transferência ou suspensão de usuários – prestadores de serviços vinculados ao contrato, principalmente se esses fatos ocorrerem antes do vencimento do contrato a que estejam vinculados, para que seus acessos sejam bloqueados.

Art. 57 - É responsabilidade das Contrapartes UFF dos contratos, divulgarem a presente norma para os terceirizados que necessitem acessar recursos de TI da UFF.

Capítulo X
Das Situações Especiais para Liberação de Acessos

Art. 58 - No caso de vencimento de contratos, provocando o bloqueio imediato de todos os recursos disponíveis, pode haver uma prorrogação dos acessos das pessoas envolvidas, nas seguintes situações.

I) Fique caracterizado que a descontinuidade do serviço contratado cause impacto direto nos interesses da UFF, comprometendo sua imagem e compromissos.

II) A prorrogação não ultrapasse 30 dias consecutivos.

III) Exista algum documento formal de prorrogação de contrato ou criação de um novo contrato.

IV) Entende-se por documento formal uma Requisição de Serviços devidamente aprovada pela área usuária, mas ainda sem processamento pelas áreas responsáveis da UFF.

V) Haja uma solicitação devidamente aprovada pelo 1º nível de reporte da área solicitante, contendo a indicação das contas de acesso (matriculas/logins), nomes e período de validade, respeitando-se o limite máximo.

VI) Em nenhum momento obterão a prorrogação, pessoas não cadastradas nos sistemas de RH e de Contratos.

VII) Não precisarão estar nos sistemas de RH e Contratos, as contas de usuários que são proprietários de objetos internos de produtos e/ou aplicações, a exemplo de Bancos de Dados e Sistemas Operacionais, que são utilizados durante instalação, atualização de versões, geração e atividades de manutenção corretiva ou evolutiva, bem como, as contas de acesso utilizadas por um sistema aplicativo que necessite estabelecer links de acesso para compartilhamento de dados. Todas as contas de acesso serão devidamente documentadas e controladas pela Área de Segurança do STI e sempre que tecnicamente possível, impedidos de serem ativados diretamente pelos usuários.

VIII) Em casos de aplicação configurada para uso público garantido através de um perfil de acesso especialmente construído e que sejam somente de consulta, serão criadas contas de acesso genéricas. Dependendo da situação e desde que aprovadas pela Área de Segurança do STI, a obrigatoriedade de senha é facultativa.

Capítulo XI
Da Utilização de E-mail

Art. 59 - As normas de utilização de e-mail, através dos recursos computacionais da Instituição englobam desde o envio, recebimento e gerenciamento de contas de e-mail. Devendo os usuários observarem os artigos que seguem:

Art. 60 - Não enviar ou repassar mensagens que abordem direta ou indiretamente, sob qualquer pretexto, racismo, discriminação, ataque pessoal, calunia, difamação, injuria ou sexo; mensagens para transacionar agiotagem, correntes, “pirâmides” de qualquer tipo e comércio de pessoa jurídica que não sejam de interesse da UFF e mensagens com fins de manifestação político-partidária, propaganda eleitoral, de associações ou sindicatos.

Art. 61 - Não utilizar e-mails com intuito de explorar pirataria de software, musicas, livros ou qualquer propriedade intelectual, pornografia, pedofilia, nudismo, armamento, drogas e artigos de descaminho ou contrabando.

Art. 62 - Ao responder mensagens externas, observar se não há nenhuma mensagem interna anexada ao e-mail e que não deva ser de conhecimento de terceiros por questões de segurança, limpando-a em caso positivo

Art. 63 - Evitar utilizar o recurso de print screen de telas colados diretamente na mensagem de e-mail

Art. 64 - É obrigatória a manutenção da caixa de correio eletrônico, evitando acumulo de mensagens e arquivos inúteis, evitando dessa forma, ultrapassar a cota máxima de armazenamento definida para cada usuário.

Art. 65 - O envio de mensagens para todos os usuários está restrito à Superintendência de Comunicação, Superintendência de Tecnologia da Informação e Reitoria. Para outros casos estas permissões serão aprovadas pela Superintendência de Comunicação e enviadas, preferencialmente em horário de menos fluxo, fracionando o envio.

Art. 66 - Além da mensagem de encerramento “Esta mensagem pode contar informações confidenciais e/ou privilegiadas. Se não for o seu destinatário, favor comunicar imediatamente ao remetente e destruir todas as informações e suas cópias” (nos idiomas português e inglês), que é disponibilizada, automaticamente pelo STI nos e-mail, o usuário deverá utilizar assinatura padronizada, com o seguinte formato:

I) Nome.
II) Função ou Área de Atuação. III) Nome da Instituição.
III) Telefone Comercial com DDD.

Capítulo XII
Da Utilização de Acesso à Internet

Art. 67 - As normas de utilização da Internet, através dos recursos computacionais da instituição, englobam desde a navegação a sites, download e upload de arquivos e está restrito às atividades necessárias para que os usuários possam desenvolver suas funções.

Art. 68 - Todos os usuários que utilizem a Internet como meio de comunicação devem fazê-lo em seu próprio nome, nunca como outra pessoa, não se admitindo o uso de qualquer outra senha a não ser a própria.

Art. 69 - É proibido utilizar os recursos da instituição para fazer download ou distribuição de software ou dados não legalizados, assim como a divulgação de informações confidenciais da instituição em grupos de discussão, listas, redes sociais, etc., não importando se a divulgação foi deliberada ou inadvertida.

Art. 70 - Os usuários com acesso à Internet não podem efetuar upload de qualquer software licenciado à instituição ou de dados de propriedade da instituição ou de seus coligados, sem expressa autorização do gestor responsável pelo software ou pelos dados.

Art. 71 - A utilização da Internet para atividades não relacionadas com os “negócios” da instituição ou realização de pesquisas e estudos para autodesenvolvimento profissional deverá ser feita dentro das regras definidas nessa política.

Art. 72 - A STI poderá gerar relatórios dos sites acessados por usuário e encaminhar ao gestor da área.

Art. 73 - Não utilizar a internet para assuntos que abordem direta ou indiretamente, sob qualquer pretexto, racismo, discriminação, ataque pessoal, calunia, difamação, injuria ou sexo; mensagens para transacionar agiotagem, correntes, "pirâmides" de qualquer tipo e com fins de manifestação político-partidária, propaganda eleitoral, de associações ou sindicatos.

Art. 74 - Não utilizar a internet com intuito de explorar pirataria de software, musicas, livros ou qualquer propriedade intelectual, pornografia, pedofilia, nudismo, armamento, drogas e artigos de descaminho ou contrabando.

Capítulo XIII
Da Utilização de Mídias Eletrônicas

Art. 75 - A aquisição e o acesso às mídias removíveis será restrito. O seu uso deve ser exclusivamente para fins de interesse da instituição e nunca para transitar informações classificadas como “confidencial” ou “reservada/restrita”, bem como, para pirataria de qualquer gênero

Capítulo XV
Do Termo de Responsabilidade e Confidencialidade

Art. 76 - Todos os colaboradores que utilizem quaisquer recursos computacionais devem, obrigatoriamente, assinar o Termo de Confidencialidade e Responsabilidade na utilização de Recursos Computacionais.

Art. 77 - O RH é o responsável pela guarda do Termo, que será anexado ao processo de cada colaborador. No caso de prestadores de serviços, a responsabilidade sobre a guarda dos Termos é da área contratante.

Capítulo XVI
Das Infrações e Penalidades

Art. 78 - Qualquer violação a qualquer uma das regras e orientações expressas nessa política, resultará em medidas disciplinares apropriadas, conforme descrito na Política de Conduta e sujeitará o usuário às penalidades administrativas e aquelas previstas nas legislações trabalhistas, civil e penal.

EMENTA: Propõe os termos da Norma de Aquisição de Recursos Computacionais da Universidade Federal Fluminense.

A Norma de Aquisição de Recursos Computacionais da Universidade Federal Fluminense tem seus termos propostos conforme segue:

Art. 1 - Quaisquer recursos que façam parte, se integrem, utilizem ou conectem ao ambiente de TI da Universidade Federal Fluminense devem exclusivamente seguir as normas de configuração, administração e controle da Superintendência de Tecnologia da Informação (STI).

Art. 2 - Recursos adquiridos mediante orçamento próprio dos órgãos constituem equipamentos da UFF e, portanto, serão administrados e controlados pela STI, devendo assim, estar de acordo com as normas e políticas desta.

Art. 3 - Recursos de propriedade particular de algum usuário necessitarão de autorização prévia e expressa da STI para que sejam conectados ao ambiente de TI da UFF. Neste caso, os mesmos também estão sujeitos às mesmas regulações que aqueles pertencentes à Instituição.

Art. 4 - Por ser parte do ambiente de TI da UFF, quaisquer recursos devem estar sujeitos a configurações por parte da STI, portanto, devem estar devidamente configurados para tal e adequados às normas da instituição.

Art. 5 - Os recursos e as informações presentes nos mesmos são de caráter institucional e estão sujeitos à monitoração por parte da STI, resguardados os garantidos pelas normas de classificação da informação e de acordo com o caso, a não divulgação dos responsáveis por parte da STI.

Capítulo I
Das Definições

Art. 6 - Para efeito dessa política considere-se:

I) **Órgão Avaliador:** é representado pela STI e tem responsabilidade de definir padrões e modelos de equipamentos, avaliar e homologar softwares, e possuir poder de veto a recursos que não estejam em concordância com o ambiente ou as normas da UFF.

II) **Usuário Solicitante:** é o usuário de qualquer área ou órgão da UFF, que identifica a necessidade e então inicia o processo de aquisição.

Capitulo II
Das Diretrizes Gerais

Art. 7 - A STI providenciará uma listagem contendo os softwares e outra os hardwares homologados para utilização no ambiente de TI da Instituição. As aquisições de soluções de TI devem obrigatoriamente priorizar os recursos constantes nestas listagens.

Art. 8 - A aquisição de recursos que não estejam presentes nas listagens de recursos homologados deverão obrigatoriamente possuir aprovação prévia da STI que verificará os seguintes itens:

I) Presença de similares em uso na Instituição, licenciados ou freewares/opensource, evitando duplicações de soluções similares e dispêndio desnecessário de recursos da instituição;

II) Adequação da solução apresentada ao ambiente de TI da Instituição, evitando incompatibilidades e possíveis falhas de segurança ou implementação;

III) Para os softwares licenciados, a existência de soluções adequadas ao usuário e opensource. Em adequação à Política de Segurança da Informação e às normas para TI na Administração Publica Federal – IN01 GSI/PR, ePing, Decreto 3.505, Lei 9.983.

Art. 9 - As soluções não presentes na listagem de homologados e aprovadas pela STI conforme Art. 2 desde documento serão catalogadas e inseridas na respectiva listagem.

Art. 10 - A STI deverá disponibilizar para consulta pública no âmbito da UFF as listagens de soluções homologadas.

Art. 11 - No caso de soluções não homologadas, a STI se responsabilizará por confeccionar o “padrão técnico” a ser anexado nos documentos de licitação.

Art. 12 - Todo o processo de homologação deverá ser documentado pelo prazo mínimo de cinco anos, incluindo documentos anexados, bem como, os “padrões técnicos” anexados às licitações.

Art. 13 - A STI esclarecerá por meio de seu serviço de HelpDesk o processo de homologação, assim como, quaisquer dúvidas relativas a aquisição de recursos computacionais.

Art. 14 - A aquisição de hardwares cujo uso destinar-se aplicações específicas que demandem software proprietário, comercial ou licenciado deve contemplar os referidos recursos. Por exemplo, a aquisição de um computador para uso de aplicações que demandem sistema operacional Windows, deve obrigatoriamente incluir nas especificações do computador a licença do sistema operacional em questão.

Capítulo II
Das penalidades e sanções

Art. 15 - A utilização de soluções não homologadas constitui infração à Política de Segurança da Informação, à Norma de Utilização de Recursos Computacionais e a diversas normas Federais, sendo, portanto passível de penalidades e sanções como as que seguem:

I) Indisponibilização em caráter temporário ou permanente do acesso ao recurso, não sendo necessário para tal prévio aviso por parte da STI.

II) Em caso de violação de patentes ou direitos autorias, a comunicação por parte da STI aos órgãos responsáveis, bem como, indicação do responsável ou responsáveis pela solução ou o ambiente no qual a mesma se encontre.

Capitulo III
Referências Normativas

Art. 16 - Este documento se ampara e referencia pelos instrumentos normativos apresentados conforme segue:

I) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

II) Lei 9.983 de 14 de julho de 2000 – Altera o Decreto-Lei nº 2.848 de 7 de dezembro de 1940 – Código Penal e dá outras providências.

III) Norma Complementar nº 10 DSIC/GSIPR – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta.

IV) Norma Complementar nº 13 DSIC/GSIPR – Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

V) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008

VI) Portaria SLTI/MP nº 05 de 14 de julho de 2005 – Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

VII) Lei 9.606 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá outras providências.

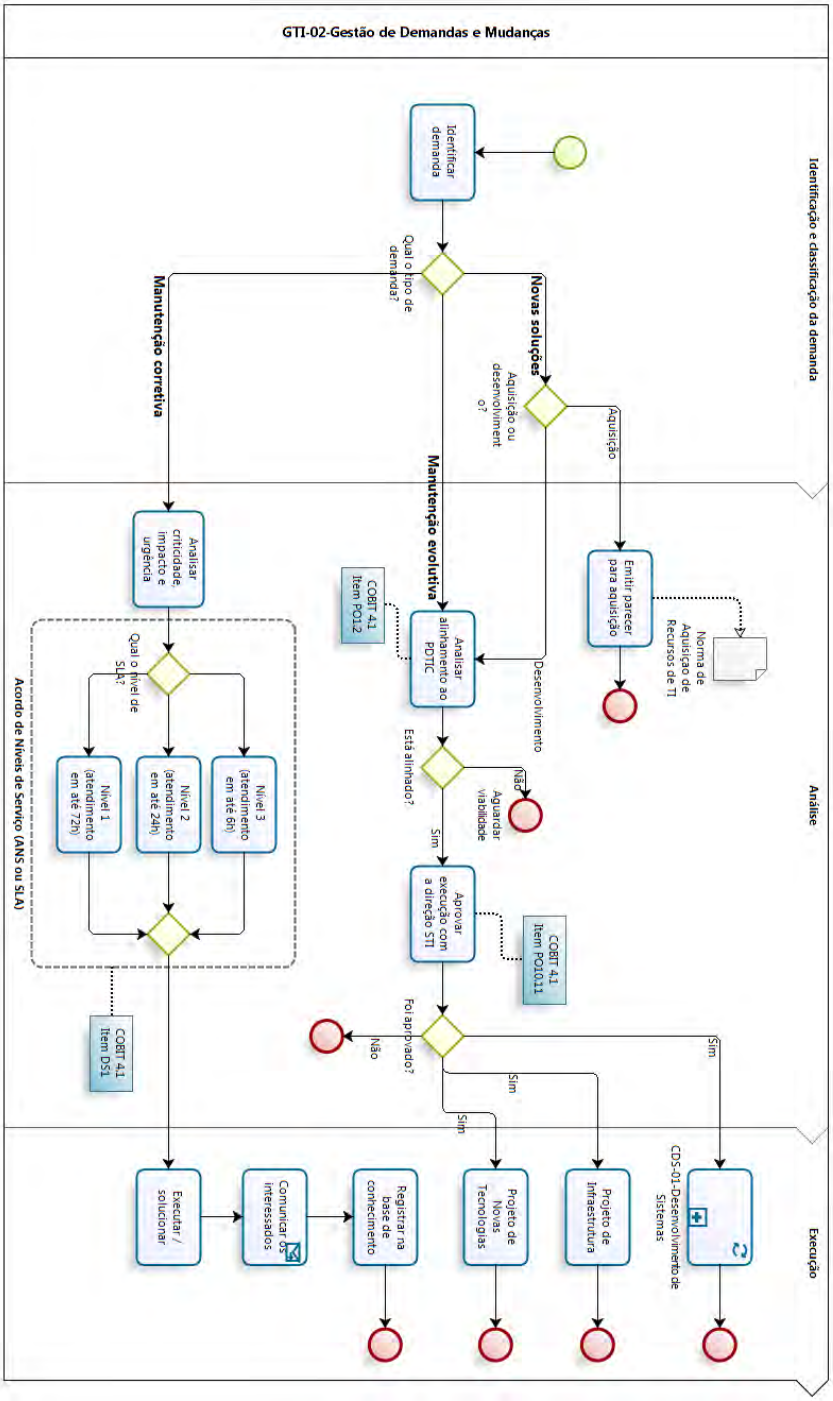
Processos de Desenvolvimento de Soluções de TI

Escritório de Gerenciamento de Projetos – PMO
Coordenação de Desenvolvimento de Sistemas
Superintendência de Tecnologia da Informação
Universidade Federal Fluminense

Versão do documento: 1.1
Niterói, 14 de dezembro de 2011

Índice

1 GTI-02-Gestão de Demandas e Mudanças
Versão: 1.0
Autor: Escritório de Gerenciamento de Projetos - STI - UFF



1.1 GTI-02-Gestão de Demandas e Mudanças

1.1.1 ELEMENTOS DO PROCESSO

Identificar demanda

Descrição

Uma demanda pode chegar à STI oriunda de:
* pró-reitorias;
* superintendências;
* outras unidades gestoras;
* reitoria.

A solicitação deve ser registrada no formulário de solicitação de mudanças ou na ferramenta oficial de gestão de informações

Solicitação de mudanças

http://www.sti.uff.br/node/add/demandas-tic

Ferramenta de gestão de informações

http://sistemas.uff.br/redmine

1.1.1.2 Qual o tipo de demanda?

Descrição

Todas as demandas e solicitações identificadas devem ser classificadas em uma das três categorias:

* Novas soluções: quando é necessário desenvolver ou adquirir uma nova solução, geralmente um sistema;
* Manutenção evolutiva: quando pretende-se acrescentar novas funcionalidades a uma solução já em produção;
* Manutenção corretiva: quando é necessário corrigir algum erro de uma solução em produção.

1.1.1.3 Aquisição ou desenvolvimento?

Descrição

Para atender às demandas por novas soluções, a STIpode desenvolver internamente uma solução ou emitir um parecer recomendando a aquisição de uma solução de outro fornecedor do mercado.

Esta decisão tem caráter técnico-gerencial e leva em consideração a disponibilidade de recursos, mão-de-obra, conhecimento e as especificidades do solicitante para desenvolver a solução.

1.1.1.4 Emitir parecer para aquisição

Descrição

A STI emite um parecer indicando a aquisição de uma solução já existente no mercado e sugere a observação do Guia de Boas de Contratação de Soluções de TI, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão.

Arquivo anexo

Guia de Boas Praticas em Contratacao de Solucoes de TI V 1.0.pdf

1.1.1.5 Analisar alinhamento ao PDTIC

Descrição

Esta análise visa verificar o alinhamento entre a demanda e o Plano de Desenvolvimento de Tecnologia da Informação e Comunicação (PDTIC) vigente. Esta atividade garante que a STI investirá seus esforços no desenvolvimento de soluções que atendam às necessidades da Universidade, mantendo-se coerente com a Política de Governança de TI da UFF.

1.1.1.6 Aguardar viabilidade

Descrição

A demanda é documentada e reavaliada na próxima revisão do PDTIC.

1.1.1.7 Aprovar execução com a direção STI

Descrição

A aprovação da direção da STI visa obter o compromisso dos gestores, que através dela iniciam um novo projeto.

1.1.1.8 CDS-01-Desenvolvimento de Sistemas

Descrição

Este diagrama descreve o processo de desenvolvimento de sistemas/soluções da STI.

Diagrama

CDS-01-Desenvolvimento de Sistemas

Processo

1.1.1.9 Analisar criticidade, impacto e urgência

Descrição

Uma análise técnica é realizada objetivando detectar o impacto, criticidade e urgência da demanda por manutenção corretiva.

* Impacto: o quanto este problema impacta na operação da solução?
* Criticidade: perguntas-chave: 1) A solução está exposta? 2) A segurança dos dados foi comprometida? 3) A operação da solução foi interrompida (saiu do ar)? Com base nestas respostas, define-se o quão crítica é a demanda.
* Urgência: perguntas-chave: a solução está em período de pico de acessos? Algum prazo do cliente está prestes a ser quebrado?

1.1.1.10 Qual o nível de SLA?

Descrição

De acordo com a análise realizada, o Nível de Serviço é determinado.

1.1.1.11 Nível 3 (atendimento em até 6h)

Descrição

Situações comuns de nível 3:

* Falhas diversas na infraestrutura de produção;
* Falhas nas rotinas de backup dos dados;
* Falhas críticas (brechas de segurança, erros de processamento dos dados) de sistemas em produção;

A solução deve ser informada a:

* Solicitante;
* Gerente do projeto em questão
* Direção da STI
* Cliente (opcional)

1.1.1.12 Nível 2 (atendimento em até 24h)

Descrição

Situações comuns de nível 2;
* Dificuldades de uso dos sistemas;
* Erros de saída de dados;

A solução deve ser informada a:
* O solicitante;
* Gerente do projeto em questão

1.1.1.13 Nível 1 (atendimento em até 72h)

Descrição

Situações comuns de nível 1:
* Erros ocasionados por falhas de uso;

A solução deve ser informada a:
* O solicitante;
* Gerente do projeto em questão (opcional)

1.1.1.14 Executar / solucionar

Descrição

Equipe responsável documenta a atividade na ferramenta de gestão de informação e soluciona o problema.

Solicitação de mudanças

http://sistemas.uff.br/redmine

1.1.1.15 Comunicar os interessados

Descrição

Após solucionar o problema, a equipe responsável comunica aos interessados, conforme o Acordo de Níveis de Serviço preestabelecido.

Implementação

Serviço Web

1.1.1.16 Registrar na base de conhecimento

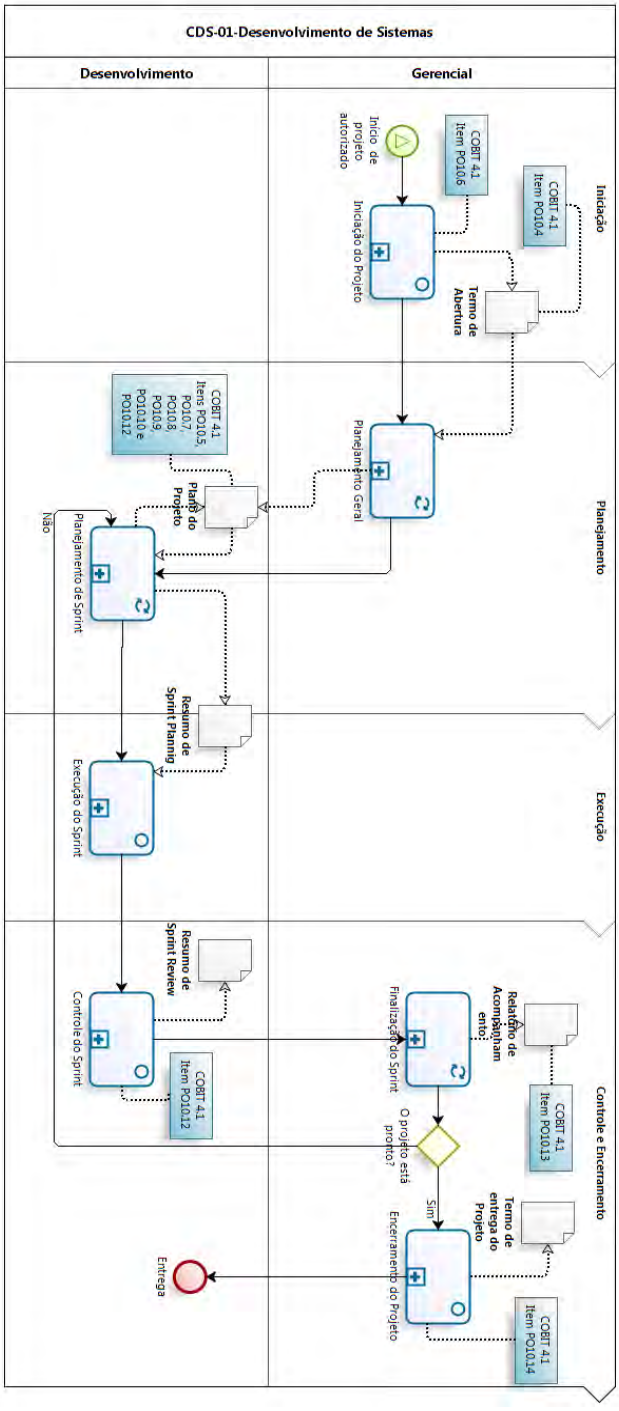
Descrição

A equipe responsável utiliza a base de conhecimento para documentar o problema e sua solução.

2 CDS-01-DESENVOLVIMENTO DE SISTEMAS

Versão: 1.1

Autor: Escritório de Gerenciamento de Projetos - STI - UFF



Descrição

Este diagrama descreve o processo de desenvolvimento de sistemas/soluções da STI.

2.1 CDS-01-DESENVOLVIMENTO DE SISTEMAS

2.1.1 ELEMENTOS DO PROCESSO

2.1.1.1 Início de projeto autorizado

Descrição

A Coordenação Desenvolvimento de Sistemas inicia um projeto quando seu início receber autorização da direção da STI.

2.1.1.2 Iniciação do Projeto

Descrição

Neste processo serão identificadas as partes interessadas, objetivo e limitações do projeto.
Ao término deste processo, o projeto efetivamente será inciado.
O marco do início do projeto é a assinatura do termo de abertura.

Executantes

PO, PMO

2.1.1.3 Planejamento Geral

Descrição

Neste processo, é feito um planejamento incial do projeto, no qual os requisitos são analisados de forma geral e superficial.

O foco deste processo é entender mais sobre o projeto com a finalidade de estimar o tamanho, custo, cronograma, equipe, Product Owner e Gerente do Projeto, e os recursos disponíveis para a sua execução. O entendimento dos requisitos deve ser suficiente apenas para estimar um cronograma básico e os definir de forma a evitar ambiguidades e futuros desentendimentos.

O principal resultado deste processo é o Plano de Gerenciamento do Projeto.

Executantes

PO, Líder do Projeto, PMO

Diagrama

Planejamento Geral

2.1.1.4 Planejamento de Sprint

Descrição

O Sprint é um ciclo de desenvolvimento de 15 dias. Ele possui um escopo definido e um objetivo estabelecido no seu planejamento, ao final dele existe uma reunião de entrega e aprovação, e uma reunião de melhoria contínua.

No processo "Planejamento de Sprint", o sprint será planejado, identificando quais requisitos devem ser entregues ao final dele. Neste processo os requisitos serão desenvolvidos e esmiuçados em tarefas, com suas respectivas estimativas. Além disso, define-se o objetivo do Sprint e toda a equipe compromete-se a trabalhar em prol dele.

O Planejamento de Sprint é dividido em duas reuniões: planejamento I e planejamento II. No primeiro planejamento, o cliente deve identificar, dentro os itens do ProducT Backlog, quais têem mais prioridade e devem ser desenvolvidos no próximo Sprint. O segundo planejmanto é uma reunião técnica, no qual a equipe irá criar tarefas para que os requisitos escolhidos possam ser entregues.

Executantes

Líder do Projeto, PO, Equipe

Diagrama

Planejamento de Sprint

Processo

2.1.1.5 Execução do Sprint

Descrição

Durante este processo a equipe efetivamente desenvolve o que foi definido no Planejamento do Sprint, ou seja, implementa cada funcionalidade para agregar valor ao produto do projeto e entregar uma parte dele ao cliente ao final de cada Sprint.

Executantes

Líder do Projeto, Equipe

2.1.1.6 Controle do Sprint

Descrição

É o processo de, entrega e homologação dos requisitos desenvolvidos ao cliente e melhoria contínua dos processos e equipe.

Os objetivos deste processo são controlar a qualidade e conformidade do que foi desenvolvido, e melhorar o processo de desenvolvimento e a capacidade técnica da equipe.

Executantes

Líder do Projeto, Equipe

2.1.1.7 Finalização do Sprint

Descrição

É o processo de acompanhamento dos resultados do trabalho da equipe.

São aferidas quatro tipos de métricas: de qualidade, do produto, de comprometimento, e de produtividade da equipe.

O resultado do Sprint de cada projeto é coletado e divulgado para que todos tenham uma visão geral do andamento dos projetos.

Executantes

PMO, Líder do Projeto

Diagrama

Finalização do Sprint

Processo

2.1.1.8 O projeto está pronto?

Descrição

O projeto é considerado pronto quando uma das condições é satisfeita:

- O objetivo identificado no termo de abertura foi alcançado;
- O Product Backlog foi entregue;

2.1.1.9 Encerramento do Projeto

Descrição

Uma vez que o que foi planejado seja plenamente implementado e entregue pela equipe ao cliente, o processo de finalização tem por finalidade averiguar se o produto do projeto atende ao escopo e qualidade definidos e tomar medidas necessárias para possíveis adequações que ainda sejam necessárias. A principal saída deste processo é o Termo de Entrega do Projeto.

Executantes

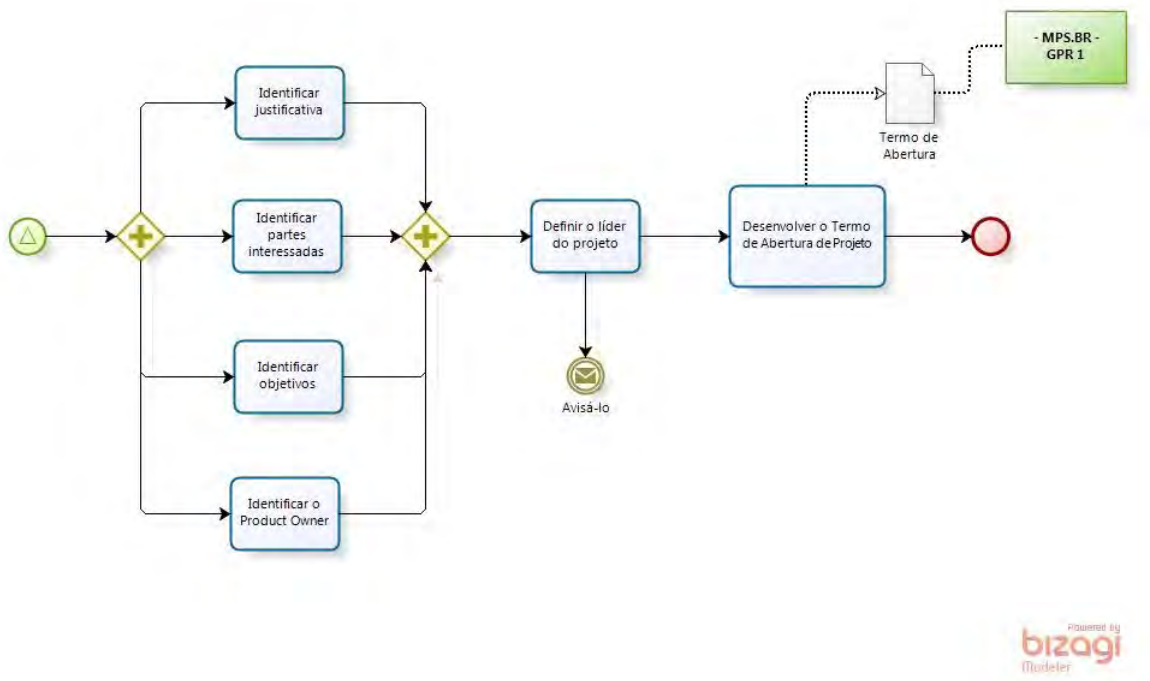
PMO, PO, Líder do Projeto

2.1.1.10 Entrega

Descrição

A entrega é o momento onde recebe o produto final do projeto como sendo o que efetivamente foi solicitado e planejado. O Termo de Entrega do Projeto é assinado e o projeto termina. A partir disto, apenas a manutenção corretiva é realizada. Novas funcionalidades não são mais desenvolvidas e aguardam a iniciação de um novo projeto caso sejam necessárias.

2.2 INICIAÇÃO DO PROJETO



Descrição

Neste processo serão identificadas as partes interessadas, objetivo e limitações do projeto.
Ao término deste processo, o projeto efetivamente será inciado.
O marco do início do projeto é a assinatura do termo de abertura.

Executantes

PO, PMO

2.2.1 ELEMENTOS DO PROCESSO

2.2.1.1 Identificar o Product Owner

Descrição

O responsável por definir a prioridade de desenvolvimento e homologar as entregas do produto deve ser identificado e registrado. O Product Owner é designado pelo cliente, ele junto ao time tem compromisso com o produto que está sendo desenvolvido e seu sucesso também depende dele. Este papel deve ser desempenhado por alguém com autonomia para responder pelos requisitos do sistema, sejam funcionais ou não funcionais.

O seu contato com a equipe ocorre em dois momentos: no Planejamento de Sprint I e na Revisão do Sprint. No planejamento ele deve definir, dentre o que ainda resta para ser desenvolvido, o que possui maior importância e será abordado no próximo Sprint. Na revisão, serão apresentados os requisitos desenvolvidos, em uma demostração no ambiente de homologação. Nesta reunião o P.O. tem o papel de validar o que foi desenvolvido e aceitar ou não. No caso de não aceitar, modificações devem ser indicadas para que sejam realizadas num próximo Sprint. Estas duas reuniões acontecem a cada 15 dias e duram entre duas e quatro horas.

O Product Owner deve estar disponível para auxiliar a equipe de desenvolvimento tirando duvidas sobre as funcionalidades desejadas quando requisitado, seja por telefone ou email. Seu papel é fundamental para o sucesso do projeto.

2.2.1.2 Desenvolver o Termo de Abertura de Projeto

Descrição

O modelo de termo e abertura utilizado pelo STI compreende os seguintes campos:

Preparador por: nome da pessoa que confeccionou o termo de abertura .

Product Owner: nome do responsável por definir a prioridade de desenvolvimento e homologar as entregas do produto. É designado pelo cliente.

Sponsor: é o cliente, o financiador do projeto.

Líder do Projeto: O responsável pelo desenvolvimento do projeto e gestão da equipe. É designado pelo Escritório de Projetos.

Partes interessadas (Stakeholders): Ver seção “Identificar as partes interessadas” logo abaixo, neste documento.

Justificativa: o motivo pelo qual o projeto deve ser feito. Pode ser acrescentado aqui a justificativa de o cliente ou o patrocinador requisitar o projeto. Podem ser incluídos também problemas de arquitetura de projetos antigos e tudo que justifique a abertura de um novo projeto (oportunidade).

Objetivos: objetivos que o projeto pretende alcançar.

Metas: Ações ou resultados a serem gerados para alcançar o objetivo em questão.

Produto do Projeto: Descreve o resultado final do projeto, aquilo que será entregue ao fim do mesmo. Isto inclui o sistema em si, suas integrações com outros sistemas, melhorias, documentos, entre outros.

Restrições: todas as limitações conhecidas ao desenvolvimento do projeto como um todo, tais como custo, tempo, limitações funcionais.

Riscos: eventos que impactam o sucesso do projeto, tanto positiva como negativamente.

Aprovado por: Nome e assinatura do responsável do PMO por este projeto e do gerente do projeto.

Ciente: Nome e assinatura do sponsor do projeto ou representante devidamente designado por este.

Data de abertura do projeto: é a data da assinatura do Termo de Abertura

2.2.1.3 Identificar justificativa

Descrição

O motivo pelo qual o projeto deve ser feito é identificado e registrado. Pode conter uma justificativa de o cliente ou o patrocinador requisitar o projeto, além de sua necessidade para a universidade. Podem ser incluídos também problemas de arquitetura de projetos antigos e tudo que justifique a abertura de um novo projeto (oportunidade).

2.2.1.4 Termo de Abertura

Descrição

O arquivo do atual modelo de Termo de Abertura utilizado pelo STI que deve ser preenchido durante este processo e assinado pelo cliente ao final do mesmo.

Arquivo anexo

Template_Termo_Abertura.doc

2.2.1.5 Identificar objetivos

Descrição

Os objetivos que o projeto pretende alcançar devem ser identificados e registrados. Estes objetivos devem ser contrastadosnos Pontos de Controle e Marcos do projeto para avaliar seu andamento e continuidade.

2.2.1.6 Identificar partes interessadas

Descrição

Todas as pessoas que possam estar envolvidas direta e indiretamente no produto final e no projeto são identificadas e registradas. Isso inclui clientes, patrocinadores, usuários, equipe de projeto, pessoas que usarão dos dados do produto produzido, entre outros.

As partes interessadas são necessárias ao planejamento do produto que deve ser desenvolvido fornecendo os pontos de vista de utilização ou de quem será afetado pelo sistema. Para garantir qualidade e usabilidade a identificação das partes interessadas é fundamental.

2.2.1.7 Definir o líder do projeto

Descrição

Cabe ao PMO definir um membro da equipe capacitado para liderar o projeto.

2.2.1.8 Avisá-lo

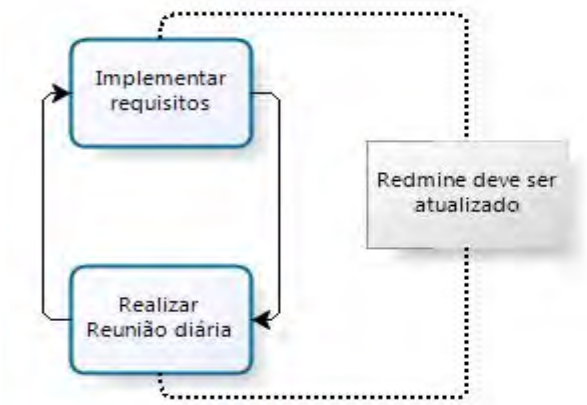
Descrição

Avisar ao membro que atuará como gerente.

Implementação

Serviço Web

2.3 EXECUÇÃO DO SPRINT



Descrição

Durante este processo a equipe efetivamente desenvolve o que foi definido no Planejamento do Sprint, ou seja, implementa cada funcionalidade para agregar valor ao produto do projeto e entregar uma parte dele ao cliente ao final de cada Sprint.

Executantes

Líder do Projeto, Equipe

2.3.1 ELEMENTOS DO PROCESSO

2.3.1.1 Implementar requisitos

Descrição

Neste processo, as ferramentas adequadas devem ser utilizadas para o desenvolvimento e implementação dos requisitos acordados na reunião de planejamento. A equipe do projeto e somente ela é responsável pela implementação dos requisitos. Caso surja algum impedimento à execução desta tarefas, ele deve ser reportado na reunião diária ou o mais breve possível ao líder do projeto.

2.3.1.2 Realizar Reunião diária

Descrição

A reunião diária é realizada no mesmo horário em cada dia e seu objetivo é acompanhar e controlar o andamento do Sprint. Nesta reunião são identificados ou reportados os impedimentos que não permitem a implementação dos requisitos ou atrapalham a produtividade da equipe de desenvolvimento.

Esta reunião deve durar no máximo 15 minutos, independente do número de membros participantes da mesma. Nela, cada membro do time de desenvolvimento deve responder a três perguntas:

1. O que foi feito desde a última reunião de acompanhamento ou planejamento de sprint, caso seja a primeira reunião;

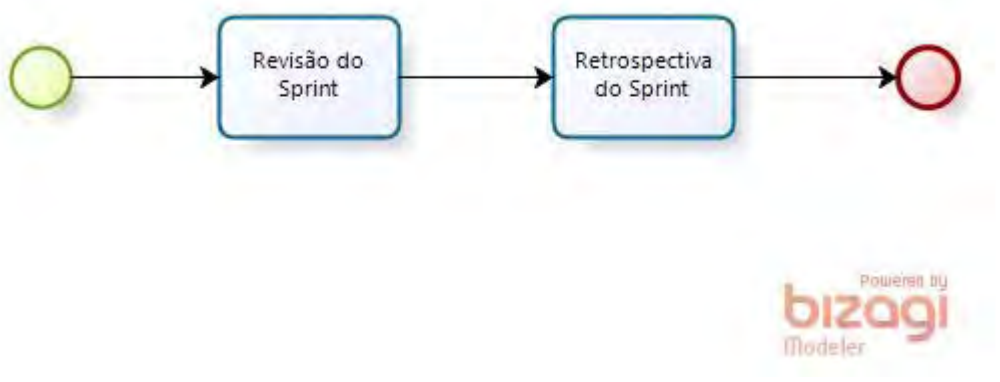
2. O que será feito até a próxima reunião de acompanhamento ou término do sprint, caso seja a última reunião;

3. Quais problemas ou impedimentos estão atrapalhando o time a implementar os requisitos.

Esta reunião deve ser realizada em pé ao lado do quadro SCRUM ou monitor com Redmine (quando o time não estiver usando um quadro SCRUM ainda). As perguntas devem ser respondidas para o time e não para o líder do projeto apenas, afinal todo o time está comprometido com os objetivos e requisitos definidos no início do Sprint.

Durante a reunião diária, cada membro deve atualizar a situação das suas tarefas no quadro SCRUM. E ao final dela, o líder do projeto deve atualizar no Redmine a situação das tarefas. Todos os membros devem ajudar o líder do projeto a manter o Redmine atualizado, com as situações das suas tarefas.

CONTROLE DO SPRINT



Descrição
É o processo de, entrega e homologação dos requisitos desenvolvidos ao cliente e melhoria contínua dos processos e equipe.

Os objetivos deste processo são controlar a qualidade e conformidade do que foi desenvolvido, e melhorar o processo de desenvolvimento e a capacidade técnica da equipe.

Executantes
Líder do Projeto, Equipe

2.4.1 ELEMENTOS DO PROCESSO

2.4.1.1 Elemento

2.4.1.2 Revisão do Sprint
Descrição
Reunião onde equipe e líder do projeto apresentam o que foi desenvolvido ao cliente já na forma de funcionalidade dentro do sistema, em ambiente de homologação.

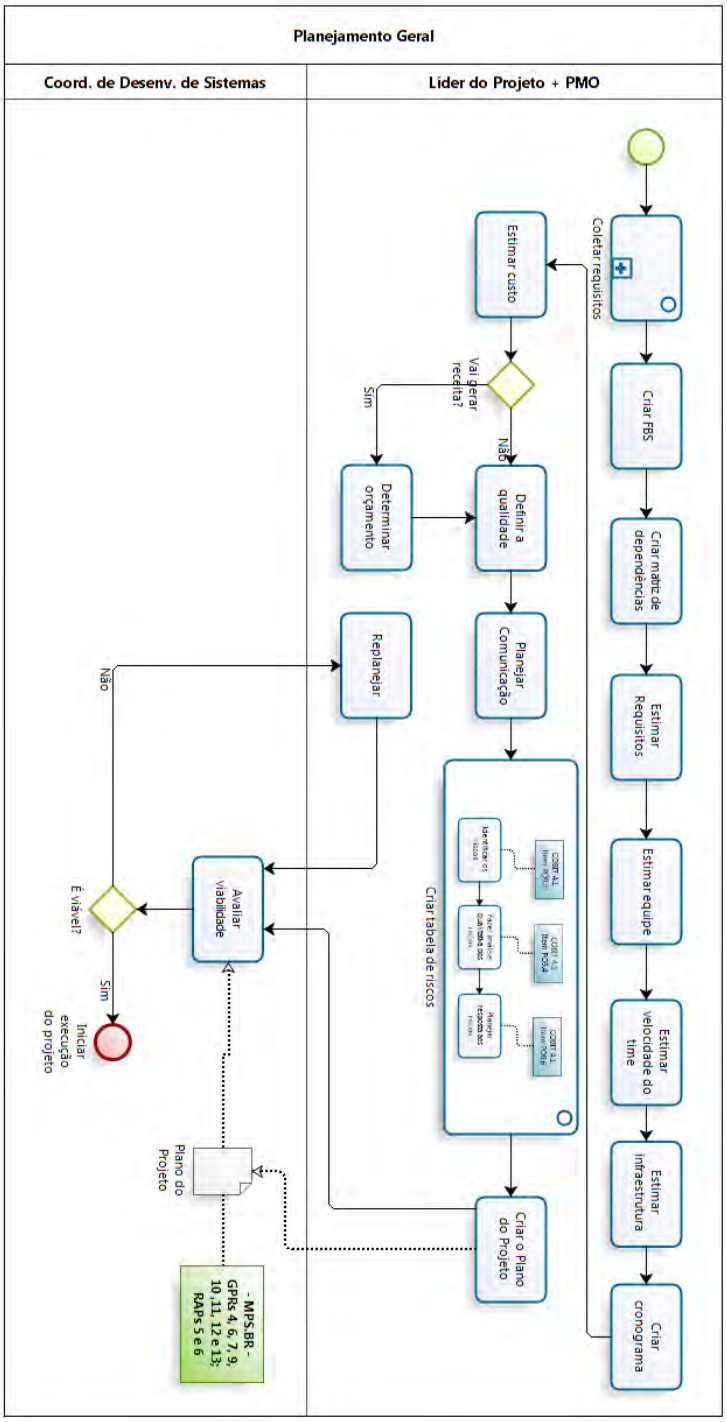
O objetivo é permitir ao cliente verificar se o que foi planejado efetivamente foi feito e validar se as entregas satisfazem às demandas.
Esta reunião deve gerar uma ata.

2.4.1.3 Retrospectiva do Sprint
Descrição
Reunião onde líder do projeto e equipe, tratam do sprint que acaba de terminar e identificam:
* O que foi bom e deve ser mantido;
* O que pode melhorar;
* Sugestões

A partir disto, todos se comprometem a esforçarem-se para atender ao que foi proposto a partir do próximo sprint.

2.4.1.4 Elemento

3 PLANEJAMENTO GERAL
Versão: 1.0
Autor: Escritório de Gerenciamento de Projetos - STI - UFF



3.1 Planejamento Geral

3.1.1 Elementos do processo

3.1.1.1 **Coletar requisitos**

Descrição

Entradas:
- Demanda inicial do cliente;
- Termo de abertura.

Ferramentas:
- Reunião de levantamento de requisitos

Saídas:
- Product Backlog, ordenado de acordo com a importância definida pelo cliente e dependências funcionais já conhecidas.

Descrição:
Um requisito deve ser escrito em linguagem de negócios e não tecnicamente, o que significa dizer, que deve conter um valor que será incorporado ao projeto ou ao produto. Além disso, deve ser entregável em no máximo um sprint. Desta forma, a cada sprint o projeto gera valor para o cliente e este valor pode ser mensurado e avaliado pelo P.O.

Todos os requisitos devem priorizar uma redação padrão, no seguinte esquema:

<Um ator> faz <alguma coisa> para <agregar algum valor>

Estes três elementos: ATOR, AÇÃO e VALOR devem sempre que possível compor a redação dos requisitos. O item “a” abaixo contém alguns exemplos disto.

Um bom requisito precisa atender às seguintes diretrizes INVEST:
I = Independente : não depende de outra história para ser concluída
N = Negociável: a qualquer momento um requisito poderá ser negociado pelo P.O.
V = Agrega Valor: obrigatoriamente precisa agregar valor ao negócio, quando for satisfeito.
E = Estimável: precisa estar minimamente detalhada e entendida a ponto da equipe conseguir realizar uma estimativa de esforço para sua conclusão;
S = Pequena (Small): precisa possuir um tamanho máximo, onde o esforço para a conclusão seja de até um Sprint;
T = Testável: precisa dizer, claramente, qual a condição para sua aceitação pelo P.O.

A coleta de requisitos é feita usualmente em dois momentos:

Reunião de levantamento de requisitos:realizada entre Product Owner (PO) e Equipe do Projeto após a assinatura do termo de abertura, esta reunião abre a fase de planejamento do projeto, e é exclusivamente destinada à coleta de requisitos. De posse do Termo de Abertura, o PO expõe mais detalhadamente suas necessidades específicas (o que chamamos histórias) e a Equipe do Projeto identifica as demandas e, lapida a informação com o PO para gerar os requisitos do projeto e do produto que devem ser contemplados na execução. Por exemplo:

O product owner diz: “preciso que o sistema controle a entrada e saída de materiais do estoque.”

O gerente identifica: registrar entrada de materiais, registrar saída de materiais, gerar relatórios sobre a movimentação.

Lapidação da informação: “Quem é o funcionário responsável pelo controle de entrada e saída de materiais? É o mesmo para os dois? O que ele faz efetivamente? Que tipo de registro ele precisa gerar? Como os gestores devem consultar estes registros?”

Identificação de requisitos:

“O estoquista deve poder cadastrar a materiais no estoque para registrar a entrada dos mesmos no patrimônio”

“O estoquista deve poder dar baixa em materiais no estoque para registrar a saída dos mesmos no patrimônio”

“Ogerente deve poder gerar relatório de entrada de materiais em estoque em um período de tempo à sua escolha para conhecer as alterações de patrimônio.”

Sprint Plannings: durante as reuniões de planejamento de cada sprint o Product Owner deve definir a ordem de desenvolvimento do produto. Dado que a cada sprint um ou mais requisitos são entregues, é comum o Product Owner apresentar outros requisitos que não havia imaginado antes.

3.1.1.2 Criar FBS

Descrição

Entradas:
- Product Baklog;

Ferramentas:
-Redmine, relatório "FBS" da seção "Tarefas" do projeto;

Saídas:
- FBS;
- Plano de projeto, seção "Estrutura analítica do projeto"

Descrição:
O formato de estrutura analítica de projeto utilizado pelo STI está orientado a funcionalidades (FBS - Features Breakdown Structure), uma vez que é mais simples para o entendimento da equipe do projeto e do próprio P.O.(cliente).
A FBS deve ser gerada através do Redmine e para que ela esteja correta é fundamental cadastrar com precisão os requisitos. Uma vez que eles estejam corretamente cadastrados basta utilizar a consulta personalizada “FBS” na guia de Tarefas do seu projeto. Ela agrupa os requisitos por categoria, gerando assim a FBS adequada.

3.1.1.3 Criar matriz de dependências

Descrição

Entradas:
- Product Backlog

Ferramentas:
- Avaliação técnica e das regras de negócio discutidas no processo de coleta de requisitos;

Saídas:
- Matriz de dependências
- Plano de projeto, seção "Matriz de dependências"

Descrição:
A matriz de dependências relaciona requisitos entre si de modo que se identifique que requisitos dependem de outros para serem implementados.

3.1.1.4 Estimar Requisitos

Descrição

Entradas:
- Product Backlog;

Ferramentas:
- Planning Poker;

Saídas:
- Product Backlog estimado;
- Plano de projeto, Seção "Product Backlog"

Descrição:
A estimativa deve ser feita em pontos de história e em alto nível, sem muitos detalhes.
Apenas o necessário para estimar o tamanho do projeto.

3.1.1.5 Estimar equipe

Descrição

Entradas:
- Product Backlog estimado;
- Termo de abertura;

Ferramentas:
- Avaliação técnico-gerencial

Saídas:
- Plano de projeto, seção "Recursos Humanos"

Descrição:
A estimativa de equipe define qual o número ideal e a capacidade das pessoas que trabalharão no projeto.

3.1.1.6 Estimar velocidade do time

Descrição

Entradas:
- Plano de projeto, seção "Recursos Humanos";
- Dados históricos;

Ferramentas:
- Avaliação técnico-gerencial
- Estimativa baseada em dados históricos

Saídas:
- Estimativa inicial de velocidade do time;
- Plano de projeto, seção "Velocidade do time"

Descrição:
A estimativa do time é feita levando em conta o número de pessoas do time e a capacidade técnica dos membros, com base em dados históricos ou em referências técnicas.

3.1.1.7 Estimar infraestrutura

Descrição

Entradas:
- Product Backlog estimado;
- Plano de projeto, seção "Recursos Humanos"

Ferramentas:
- Avaliação tecnico-gerencial;

Saídas:
- Plano de projeto, seção "Infraestrutura"

Descrição:
Com base no que precisa ser desenvolvido e na e equipe que particiará deste desenvolvimento, é realizada uma avaliação técnico-gerencial objetivando estimar infraestrutura necessária ao projeto. A partir desta avaliação serão identificadas necessidades como espaço de trabalho,máquinas, ferramentas, tecnologias, mobiliário, espaço de disco, capacidade de processamento e memória dos servidores, sistema de controle de versões e tudo o mais que for preciso para garantir à equipe as condições de desenvolvimento do projeto.

3.1.1.8 Criar cronograma

Descrição

Entradas:
- Plano de projeto, seção "Product Backlog";
- Plano de projeto, seção "Velocidade do time";
- Plano de projeto, seção "Matriz de dependências".

Feramentas:
- Estimativa com fator de foco/produtividade;
- Divisão de tempo em sprints

Saídas:
- Cronograma baseado em sprints;
- Plano de projeto, seção "Cronograma".

Descrição:
Distribuir os itens do backlog em sprints, de acordo com a velocidade do time, respeitando a ordem de importância dos requisitos definida pelo cliente e possíveis dependências entre eles.

3.1.1.9 Estimar custo

Descrição

Entradas:
- Plano de projeto, seção "Recursos Humanos";
- Plano de projeto, seção "Cronograma";
- Plano de projeto, seção "Infraestrutura".

Ferramentas:
- Avaliação financeira
- Planilha de estimativas

Saídas:
- Planilha de estimativa de custos do projeto

Descrição:
A partir da análise das estimativas de recursos humanos, da infraestrutura e do tempo necessários ao desenvolvimento do projeto, estima-se o custo total do mesmo em uma planilha de estimativa.

3.1.1.10 Determinar orçamento

Descrição

Entradas:
- Estimativa de custo;

Ferramentas:
- Avaliação gerencial

Saídas:
- Orçamento do projeto

Ddescrição:
Se o projeto for gerar receita, é necessário definir um preço com base no custo estimado.

3.1.1.11 Definir a qualidade

Descrição

Entradas:
- Termo de Abertura do Projeto
- Produc Backlog Estimado

Ferramentas:
- Avaliação técnico-gerencial

Saídas:
- Indicadores e metas de qualidade

Descrição

Alguns indicadores de qualidade são padronizados, independente do projeto. São eles:
* 80% de cobertura mínima de código;
* 100% de testes passando.

Caso necessário, outros indicadores podem ser definidos.

3.1.1.12 Planejar Comunicação

Descrição

Toda a execução do projeto em seus diversos ciclos (sprints) é documentada e levada ao conhecimento de toda a equipe e cliente.
As reuniões de planejamento e revisão de sprint são registradas em atas, que são armazenadas pelo PMO.

3.1.1.13 Criar tabela de riscos

Descrição

Entradas:
- Termo de Abertura;
- Cronograma;
- Estimativa de equipe;
- Estimativa de custos;
- Estimativa de infraestrutura.

Ferramentas:
- Avaliação gerencial

Saídas:
- Tabela de riscos

Descrição:
Os riscos devem ser identificados e catalogados na tabela de riscos, contendo uma descrição, uma análise qualitativa e um planejamento de resposta à cada risco.

3.1.1.14 Criar o Plano do Projeto

Descrição
Entradas:
- Termo de abertura;
- Template de plano de projeto;

Saídas:
- Plano de Projeto

Descrição:
Com base nas saídas de cada atividade deste processo, o plano de projeto é apenas organizado utilizando o template padrão de plano de projeto, fornecido pelo Escritório de Projetos.

3.1.1.15 Avaliar viabilidade

Descrição
Entradas:
- Plano de Projeto

Ferramenta:
- Avaliação gerencial

Saídas:
- Plano de projeto aprovado

Descrição:
O Diretor de Desenvolvimento de Sistemas deve avaliar o Plano de Projeto em todos os seus aspectos e julgar se é viável a execução do mesmo da forma como foi planejado.
Se aprovado, o projeto está apto a ser iniciado.
Se não aprovado, ele deve observar que aspectos não estão adequados e enviar para o replanejamento.

3.1.1.16 Replanejar

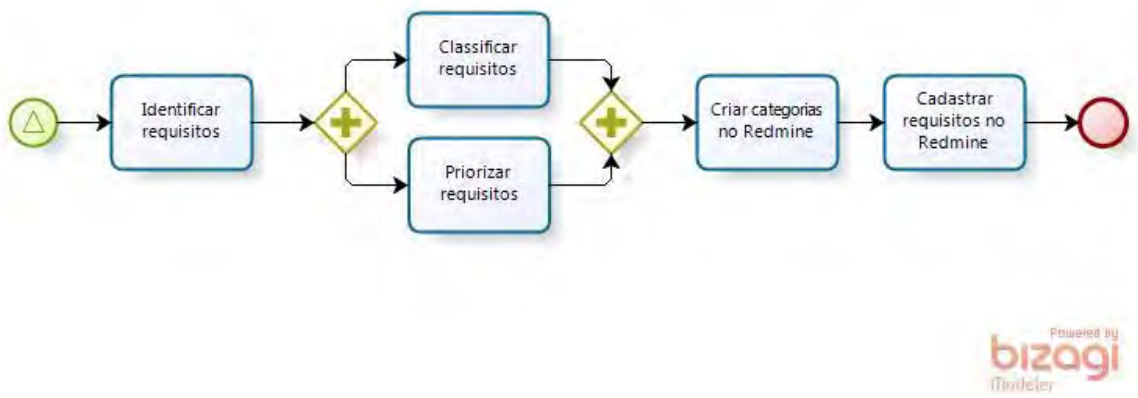
Descrição
Entradas:
- Plano de projeto;
- Observações sobre inadequações no plano de projeto.

Ferramentas:
- Reavaliação dos aspectos considerados inadequados.

Saídas:
- Plano de Projeto revisado

Descrição:
Com base nas observações feitas pelo Diretor de Desenvolvimento de Sistemas o líder de projeto deve reexecutar as atividades relativa às inadequações corrigindo os aspectos necessários. Depois disso o plano deve ser reenviado ao Diretor para nova avaliação.

3.2 Coletar requisitos



Descrição
Entradas:
- Demanda inicial do cliente;
- Termo de abertura.

Ferramentas:
- Reunião de levantamento de requisitos

Saídas:
- Product Backlog, ordenado de acordo com a importância definida pelo cliente e dependências funcionais já conhecidas.

Descrição:
Um requisito deve ser escrito em linguagem de negócios e não tecnicamente, o que significa dizer, que deve conter um valor que será incorporado ao projeto ou ao produto. Além disso, deve ser entregável em no máximo um sprint. Desta forma, a cada sprint o projeto gera valor para o cliente e este valor pode ser mensurado e avaliado pelo P.O.
Todos os requisitos devem priorizar uma redação padrão, no seguinte esquema:

<Um ator> faz <alguma coisa> para <agregar algum valor>
Estes três elementos: ATOR, AÇÃO e VALOR devem sempre que possível compor a redação dos requisitos. O item “a” abaixo contém alguns exemplos disto.

Um bom requisito precisa atender às seguintes diretrizes INVEST:

I = Independente : não depende de outra história para ser concluída
N = Negociável: a qualquer momento um requisito poderá ser negociado pelo P.O.
V = Agrega Valor: obrigatoriamente precisa agregar valor ao negócio, quando for satisfeito.
E = Estimável: precisa estar minimamente detalhada e entendida a ponto da equipe conseguir realizar uma estimativa de esforço para sua conclusão;
S = Pequena (Small): precisa possuir um tamanho máximo, onde o esforço para a conclusão seja de até um Sprint;
T = Testável: precisa dizer, claramente, qual a condição para sua aceitação pelo P.O.

A coleta de requisitos é feita usualmente em dois momentos:

Reunião de levantamento de requisitos: realizada entre Product Owner (PO) e Equipe do Projeto após a assinatura do termo de abertura, esta reunião abre a fase de planejamento do projeto, e é exclusivamente destinada à coleta de requisitos. De posse do Termo de Abertura, o PO expõe mais detalhadamente suas necessidades específicas (o que chamamos histórias) e a Equipe do Projeto identifica as demandas e, lapida a informação com o PO para gerar os requisitos do projeto e do produto que devem ser contemplados na execução. Por exemplo:

O product owner diz: “preciso que o sistema controle a entrada e saída de materiais do estoque.”

O gerente identifica: registrar entrada de materiais, registrar saída de materiais, gerar relatórios sobre a movimentação.

Lapidação da informação: “Quem é o funcionário responsável pelo controle de entrada e saída de materiais? É o mesmo para os dois? O que ele faz efetivamente? Que tipo de registro ele precisa gerar? Como os gestores devem consultar estes registros?”

Identificação de requisitos:

“O estoquista deve poder cadastrar a materiais no estoque para registrar a entrada dos mesmos no patrimônio”

“O estoquista deve poder dar baixa em materiais no estoque para registrar a saída dos mesmos no patrimônio”

“O gerente deve poder gerar relatório de entrada de materiais em estoque em um período de tempo à sua escolha para conhecer as alterações de patrimônio.”

Sprint Plannings: durante as reuniões de planejamento de cada sprint o Product Owner deve definir a ordem de desenvolvimento do produto. Dado que a cada sprint um ou mais requisitos são entregues, é comum o Product Owner apresentar outros requisitos que não havia imaginado antes.

3.2.1 ELEMENTOS DO PROCESSO

3.2.1.1 Elemento

3.2.1.2 Criar categorias no Redmine

Descrição

Para cadastrar categorias no Redmine você deve ser o líder do seu projeto.
Basta clicar na em “Configurações” >> “Categorias das tarefas” e em seguida clicar no botão “Nova categoria” do lado esquerdo da tela.
Depois de clicar no botão “Nova categoria” , basta digitar o nome da categoria e criar. Não é necessário preencher o campo “Atribuído para”.

3.2.1.3 Identificar requisitos

Descrição

A coleta de requisitos é feita usualmente em dois momentos: levantamento inicial de requisitos e Sprint Planning.

Reunião de levantamento de requisitos:

realizada entre Product Owner (PO) e Equipe do Projeto após a assinatura do termo de abertura, esta reunião abre a fase de planejamento do projeto, e é exclusivamente destinada à coleta de requisitos. De posse do Termo de Abertura, o PO expõe mais detalhadamente suas necessidades específicas (o que chamamos histórias) e a Equipe do Projeto identifica as demandas e, lapida a informação com o PO para gerar os requisitos do projeto e do produto que devem ser contemplados na execução. Por exemplo:

O product owner diz: “preciso que o sistema controle a entrada e saída de materiais do estoque.”

O gerente identifica: registrar entrada de materiais, registrar saída de materiais, gerar relatórios sobre a movimentação.

Lapidação da informação: “Quem é o funcionário responsável pelo controle de entrada e saída de materiais? É o mesmo para os dois? O que ele faz efetivamente? Que tipo de registro ele precisa gerar? Como os gestores devem consultar estes registros?”

Identificação de requisitos:

“O estoquista deve poder cadastrar a materiais no estoque para registrar a entrada dos mesmos no patrimônio”

“O estoquista deve poder dar baixa em materiais no estoque para registrar a saída dos mesmos no patrimônio”

“Ogerente deve poder gerar relatório de entrada de materiais em estoque em um período de tempo à sua escolha para conhecer as alterações de patrimônio.”

Sprint Plannings:

Durante as reuniões de planejamento de cada sprint o Product Owner deve definir a ordem de desenvolvimento do produto. Dado que a cada sprint um ou mais requisitos são entregues, é comum o Product Owner apresentar outros requisitos que não havia imaginado antes.

3.2.1.4 Classificar requisitos

Descrição
A partir da coleta de requisitos, obtemos uma listagem das funcionalidades que devem ser entregues - a isto damos o nome de Product Backlog (PB). De posse do PB, precisamos agrupar os requisitos de acordo com suas características, de modo que o PB fique mais organizado e fácil de se entender e, ainda mais importante, para que possamos criar a EAP.
Imaginemos os seguintes requisitos:

"O estoquista deve poder cadastrar a materiais no estoque para registrar a entrada dos mesmos no patrimônio";

"O estoquista deve poder dar baixa em materiais no estoque para registrar a saída dos mesmos no patrimônio";

"Ogerente deve poder gerar relatório de entrada de materiais em estoque em um período de tempo à sua escolha para conhecer as alterações de patrimônio";

"O gerente deve poder gerar relatório de listagem de materiais em estoque por categoria, para controlar o abastecimento da empresa";

"O gerente deve poder cadastrar fornecedores para manter uma base de consulta de fornecedores de materiais";

"O gerente deve poder visualizar fornecedores ordenados por data de inclusão ou por última transação realizada, para obter informações sobre os fornecedores mais antigos ou mais frequentes".

Repare que os requisitos a e b referem-se a operações com materiais. Assim, poderíamos agrupá-los numa categoria chamada “Materiais”.
Do mesmo modo, os requisitos c e d tratam da geração de relatórios. Logo, agrupar-se-iam na categoria “Relatórios”.

Analogamente, os requisitos e e f pertenceriam à categoria “Fornecedores”.

IMPORTANTE: Cabe ressaltar que a classificação de requisitos em categorias não é um procedimento único e invariável. Existem diversas maneiras de classificar requisitos e nenhuma está absolutamente correta ou incorreta. Elas servem, de modos diferentes, ao mesmo objetivo: tornar a estrutura geral do sistema mais inteligível e orientar o desenvolvimento à construção de valor, e não apenas à criação de código. Uma outra classificação para os requisitos anteriores poderia ser:

Os requisitos a e b referem-se ao ator “estoquista”;
Os requisitos c, d, e e f referem-se ao ator “gerente”;

Cada cliente traz demandas e prioridades distintas, às quais uma determinada classificação atende melhor que outra, ou ainda uma terceira, diferente das duas anteriores. A categorização pode depender da demanda, do cliente, do sistema, do público-alvo, etc. Independente de como se ela dá, o importante é que ela reflita a realidade e seja coerente com o que foi acordado com o cliente.

3.2.1.5 Cadastrar requisitos no Redmine

Descrição

Após a criação das categorias de requisitos, cada um deles deve ser cadastrado e incluído em uma categoria, sempre seguindo a escrita padrão de requisitos.

3.2.1.6 Priorizar requisitos

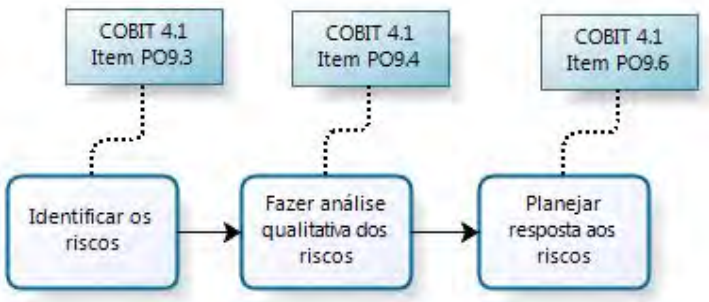
Descrição

Esta é a atividade em que o P.O. estabelece uma pontuação de importância de cada requisito, com o intuito de definir uma ordem de implementação. Com base nesta pontuação a equipe desenvolve as funcionalidades para o sistema. A pontuação dada a cada requisito estabelece apenas a ordem de execução, não uma relação numérica entre eles. Por exemplo: Se o requisito A possui importância10 e o B possui importância 30, não significa que B é 3 vezes mais importante que A (dado que 3x10=30), mas simplesmente que B é mais importante que A.

Executantes

PO, Líder do Projeto, Equipe

3.3 CRIAR TABELA DE RISCOS



Descrição
Entradas:
- Termo de Abertura;
- Cronograma;
- Estimativa de equipe;
- Estimativa de custos;
- Estimativa de infraestrutura.

Ferramentas:
- Avaliação gerencial

Saídas:
- Tabela de riscos

Descrição:
Os riscos devem ser identificados e catalogados na tabela de riscos, contendo uma descrição, uma análise qualitativa e um planejamento de resposta à cada risco.

3.3.1 ELEMENTOS DO PROCESSO

3.3.1.1 Identificar os riscos

Descrição

Identificar eventos com potencial impacto negativo nos objetivos ou nas operações da organização, incluindo aspectos de negócios, regulamentação, aspectos jurídicos, tecnologia, parcerias de negócio, recursos humanos e operacionais. Determinar a natureza do impacto e manter esta informação.

3.3.1.2 Planejar resposta aos riscos

Descrição

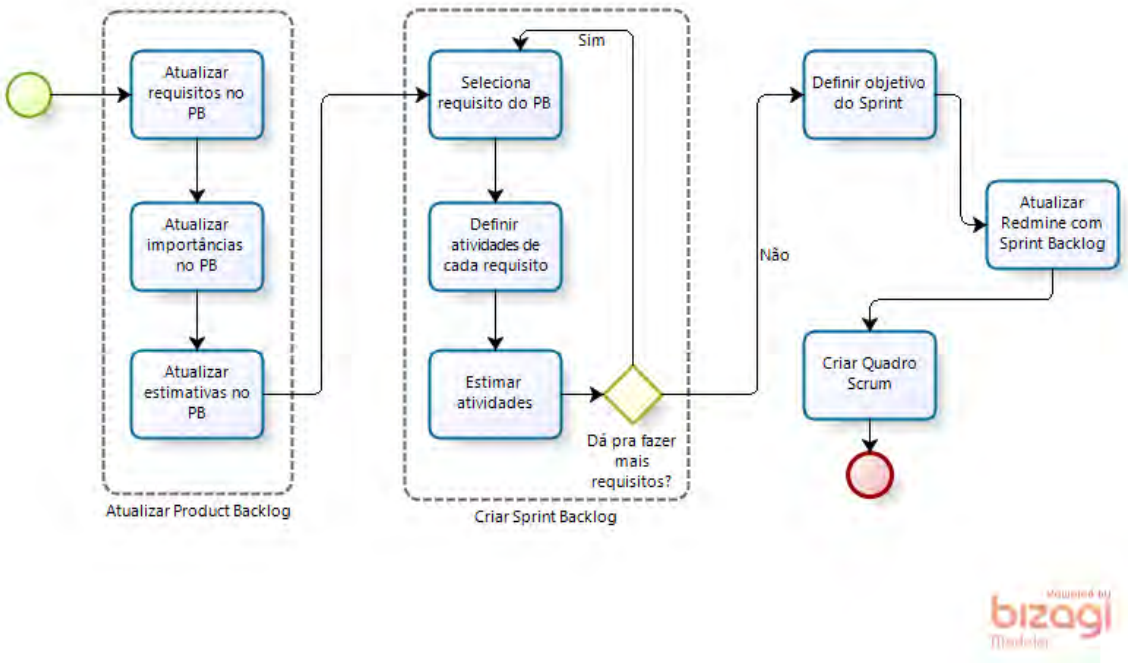
Desenvolver e manter um planejamento de resposta aos riscos. A resposta ao risco deve identificar estratégias de risco e considerar os níveis de tolerância definidos.

3.3.1.3 Fazer análise qualitativa dos riscos

Descrição

Analisar a probabilidade e o impacto de todos os riscos identificados, utilizando métodos qualitativos.

4 Planejamento de Sprint
Versão: 1.0
Autor: STI



4.1 Processo principal

4.1.1 ELEMENTOS DO PROCESSO

4.1.1.1 Atualizar requisitos no PB

Descrição

Na reunião de planejamento do sprint deve-se conhecer, tanto quanto possível, os objetivos de requisito, o valor de negócio, observações importantes acerca da implementação e tudo o mais que for necessário para garantir que a equipe conseguirá definir como implementar o requisito.

4.1.1.2 Atualizar importâncias no PB

Descrição

O cliente deve priorizar os requisitos de acordo com o valor de cada um para o negócio. Esta estimativa deve ser registrada nos requisitos no Redmine.

4.1.1.3 Atualizar estimativas no PB

Descrição

A equipe e o líder de projeto devem analisar as informações existentes de um requisito e estimá-lo utilizando o planning poker.

4.1.1.4 Seleciona requisito do PB

4.1.1.5 Definir atividades de cada requisito

Descrição

Entradas:
- Product Backlog

Ferramentas:
- Planning Poker
- Estimativa em pontos de complexidade

Saídas:
- Tarefas cadastradas e estimadas no Redmine.

Descrição:
É a identificação das tarefas especficas necessárias para entregar os requisitos. Requisitos definem O QUE deve ser feito. Tarefas dizem COMO fazer.

Referências
- [PMBOK:6.1 Definir Atividades]
- Ferramenta do PMBOK: Planejamento em ondas sucessivas

4.1.1.6 Estimar atividades

Descrição

Entradas:
* Lista de atividades de cada requisito que será implantado no próximo sprint.

Ferramentas:
- Planning Poker
- Estimativa em pontos de complexidade

Saídas:
- Tarefas cadastradas e estimadas no Redmine.

Descrição:
É a estimativa de quanto esforço será necessário para concluir cada atividade. Esta estimativa não é feita em tempo, mas em Pontos de Complexidade, que leva em conta o conhecimento necessário e o que se possui sobre a tecnologia e as regras para realizar a atividade, o tempo que toma, a complexidade de execução, entre outros.

Referências:

4.1.1.7 Definir objetivo do Sprint

Descrição

O objetivo do sprint deve responder perguntas fundamentais “Por que nós estamos fazendo este sprint? O que queremos conquistar com ele?"

4.1.1.8 Atualizar Redmine com Sprint Backlog

Descrição

As informações dos selecionados para o sprint e das tarefas estimadas, devem ser atualizadas no redmine, registrando o Sprint backlog.

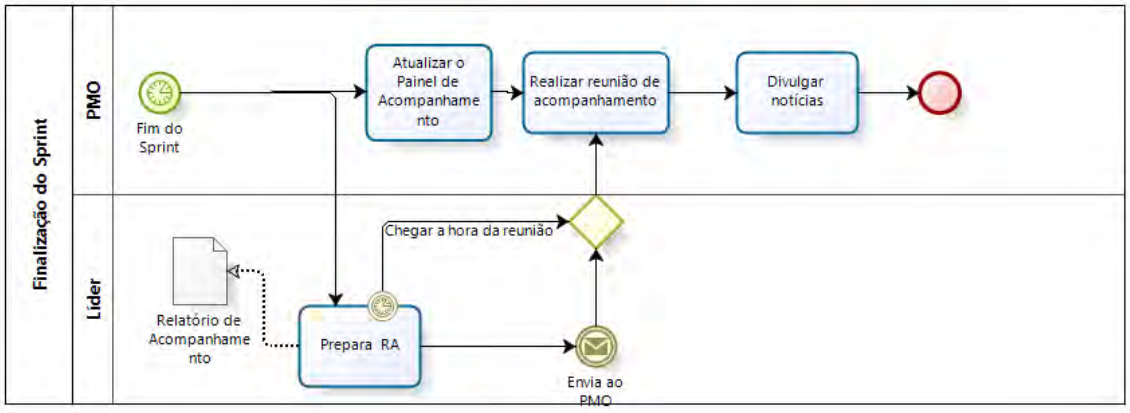
4.1.1.9 Criar Quadro Scrum

Descrição

Dado que todos os requisitos e respectivas tarefas já foram atualizados no Redmine, deve-se imprimi-los e anexar no quadro Scrum.
Este quadro será ferramenta importante na execução do sprint, especialmente nas reuniões diárias.

5 FINALIZAÇÃO DO SPRINT

Versão: 1.0
Autor: Daniel



5.1 FINALIZAÇÃO DO SPRINT

5.1.1 ELEMENTOS DO PROCESSO

5.1.1.1 Prepara RA

Descrição

O gerente do projeto deve preencher o Relatório de Acompanhamento, com base no template disponibilizado pelo PMO.

Arquivo anexo

Template_RA_v3.5.doc

5.1.1.2 Realizar reunião de acompanhamento

Descrição

A Reunião de Acompanhamento é realizada entre PMO e gerente do projeto, orientada pela discussão de cada item do relatório de acompanhamento. É um ponto importante de checagem do cumprimento do processo e de identificação de demandas que precisem do apoio direto do PMO na sua solução.

5.1.1.3 Divulgar notícias

Descrição

As notícias coletadas nas reuniões de acompanhamento passam por uma triagem do PMO e são divulgadas apenas internamente ou interna e externamente, pela equipe de mídia e supervisionadas pelo PMO.

5.1.1.4 Atualizar o Painel de Acompanhamento

Descrição

O painel de acompanhamento contém os indicadores de cada projeto em execução e é atualizado com dados extraídos via banco de dados do Redmine. O painel é atualizado a cada sprint e disponibilizado via web.

6 PARTICIPANTES

RHB (Função)

O setor de Recursos Humanos de Bolsistas tem a função de executar recrutamento e seleção de bolsistas e controle da alocação de cada bolsista nos projetos

Líder do Projeto (Função)

O líder é a referência de processo e metodologia da equipe. Cada equipe de desenvolvimento precisa possuir um líder, e este é o principal ponto de contato de cada equipe com o PMO. O líder é o responsável por conduzir as reuniões internas da equipe com o cliente, garantir que os desenvolvedores possuam as condições necessárias para executar seu trabalho e remover possíveis impedimentos que surjam durante os sprints (ciclos de desenvolvimento).

Membro (Função)

O Membro é qualquer integrante do STI

PMO (Função)

PMO é a sigla em inglês para Escritório de Gerenciamento de Projetos. Esta é a equipe responsável pela definição e manutenção dos padrões de processos e métricas e pelo suporte ao gerenciamento dos projetos. As principais funções do PMO são:

Gestão dos recursos compartilhados entre os projetos;

Orientação, aconselhamento, supervisão e treinamento das equipes;

Coordenação da comunicaçãoentre projetos

PO (Função)
O Product Owner é pessoa responsável pela definição e gerenciamento das funcionalidades que serão desenvolvidas e por garantir o valor do trabalho realizado pelo Time. Essa pessoa define em que ordem os requisitos devem ser implementados e garante que todos saibam em que devem trabalhar.
Ao final de cada Sprint, o product owner homologa as funcionalidades desenvolvidas pelo time.
Referência: Scrum Guide, 02/2010

Equipe (Função)
É o grupo de desenvolvedores, que transformam os requisitos em incrementos de funcionalidades a cada Sprint. As equipes devem ser multidisciplinares e auto-organizáveis, na medida em que devem definir como cada requisito deve ser implementado e possuir as habilidades necessárias ao seu desenvolvimento.

Indicadores de desempenho

Valor para a UFF

Quantidade de visitas únicas por sistema

Produtividade
- Quantidade de requisitos planejados
- Quantidade de requisitos entregues
- Quantidade de requisitos não entregues
- Quantidade de tarefas planejadas
- Quantidade de tarefas entregues
- Quantidade de tarefas não entregues
- Tamanho da equipe

Qualidade
- Cobertura unitária de código
- Quantidade de testes unitários
- Quantidade de problemas reportados
- Quantidade de problemas em aberto

Aderência ao processo
- Quantidade de requisitos estimados
- Quantidade de requisitos não estimados
- Quantidade de tarefas estimadas
- Quantidade de tarefas não estimadas
- Quantidade de horas trabalhadas
- Quantidade de horas esperadas e faltantes

8 ANEXOS

Modelos padronizados

Anexo 1 - Termo de Abertura de Projeto
Anexo 2- Plano de Projeto
Anexo 3- Resumo de Sprint Planning
Anexo 4 - Resumo de Sprint Review
Anexo 5 - Relatório de Acompanhamento

Imagens:

Anexo 6 - Painel de Acompanhamento

ANEXO 1

[Nome e sigla do projeto]		
TERMO DE ABERTURA DO PROJETO		
Preparado por:	[Nome da pessoa que preparou o documento]	Versão 1.0
Product Owner:	[Nome do cliente do projeto]	
Cliente/Sponsor:	[Nome do patrocinador do projeto]	
Gerente do projeto:	[Nome do gerente do projeto]	
PMO:	[Nome do PMO responsável no acompanhamento do projeto]	

Partes Interessadas (Stakeholders)
[Partes interessadas ao projeto. Todas as pessoas que possam estar envolvidas direta e indiretamente no produto final a ser desenvolvido pelo projeto. Isso inclui clientes, patrocinadores, usuários, equipe de projeto, pessoas que usarão dos dados do produto produzido, etc.]

Justificativa
[Justificativa do porque o projeto deve ser feito. Pode ser acrescentado aqui a justificativa pela qual o cliente ou o patrocinador requisitou o projeto. Podem ser incluídos também problemas de arquitetura de projetos antigos e tudo que justifique a abertura de um novo projeto (oportunidade)].

Objetivos	**Metas**
[Objetivo do projeto. Podem existir vários objetivos para esse projeto]	[Meta a ser alcançada a partir do objetivo do projeto. Podem existir várias metas para um mesmo objetivo].

Produto do Projeto
[Aqui deve ser descrito o produto que será gerado a partir desse projeto. Isto inclui o sistema em si, suas integrações com outros sistemas, melhorias, documentos entre outros.]

Restrições
[Restrições que podem ser encontradas pelo projeto. Coisas que limitam ou podem limitar o desenvolvimento do projeto]

Riscos
[Riscos positivo e risco negativos ao projeto devem ser apontados nesse tópico.]

Aprovado por:		
Nome	**Papel**	**Assinatura**
[Nome do responsável pelo projeto (Patrocinador ou representante do patrocinador]	Sponsor	

Ciente:		
Nome	**Papel**	**Assinatura**
[Nome do PMO do projeto]	PMO	
[Nome do gerente de projetos]	Gerente do Projeto	

Data de Abertura do Projeto	**XX de XXXXXXX de 2011.**

ANEXO 2

[Digite o nome do Projeto]		
PLANO DO PROJETO		
Preparado por	[Nome do responsável pelo documento]	Versão [Versão]
Aprovado por	[Nome do responsável pela aprovação]	[Data]

Informações gerais

Data de Início	[Data de início do Projeto]
Data de Término	[Data de término do projeto]

Escopo

a. Estrutura Analítica do Projeto (FBS)

[Coloque aqui a Estrutura Analítica do Projeto. É o relatório "**FBS**" do Redmine.]

b. Product Backlog

[Product Backlog extraído do Redmine]

c. Matriz de Dependências

Recursos Humanos

PAPÉIS	
NOME	**DESCRIÇÃO**
[Nome do papel]	[Descrição das responsabilidades e atribuições do papel]

RECURSOS HUMANOS DO PROJETO				
Nome	**Papel**	**Carga Horária** (Semanal)	**Contato**	
			Telefone	**E-mail**
[Nome do membro]	[Papel]	[horas semanais]	[telefone]	[email]

CAPACIDADE DE PRODUÇÃO	[Quantos pontos de complexidade a equipe rende por sprint]

Comunicação

Armazenamento dos documentos	
Disseminação de informações	

Qualidade

IDENTIFICAÇÃO	**AVALIAÇÃO DE QUALIDADE**
Testes automatizados	100% dos testes passando com Cobertura mínima de 80%
Complexidade do código	Complexidade ciclomatica média abaixo de 15

Riscos

[Matriz de Riscos categorizados qualitativamente. Os riscos na matriz devem estar ordenados decrescentemente pela exposição. A Probabilidade e o Impacto são valores numéricos de 1 a 10 e a exposição é a multiplcação dos dois valores anteriores.]

MATRIZ DE RISCOS					
Risco	**Exposição**	**Probabilidade**	**Impacto**	**Contenção**	**Contingência**
[Descrição do risco]	[Prob. x Impac.]	[Chance de ocorrer o risco]	[Impacto desse risco para o sucesso do projeto]	[O que pode ser feito para mitigar o risco?]	[O que será feito se o risco se tornar verdade?]

Cronograma

[O cronograma deve relacionar quais requisitos devem ser entregues em quais sprints. É o relatório "**Cronograma(PB por sprints)**" do Redmine].

MARCOS E PONTOS DE CONTROLE			
Evento	**Data**	**Presentes**	**Objetivo**
[nome do evento]	[dia/ mes / ano]	[quem deve estar presente?]	[qual o objetivo desse evento?]

Aprovado por:		
Nome	**Papel**	**Assinatura**
[Nome do Cliente/Sponsor]	Sponsor	
[Nome do responsável do PMO]	PMO	

Data de aprovação do Plano:	**XX de XXXXXXXXX 2011.**

ANEXO 3

[Nome e sigla do projeto]
RESUMO DO SPRINT PLANNING - [Código do Sprint]

PARTICIPANTES	
Scum Master:	
Product Owner:	
Scrum Team:	
Outros:	

OBJETIVO DO SPRINT

REQUISITOS SELECIONADOS		
# Ticket	**Título**	**Observação**

Data:	/ /	**Sprint:**	
Assinatura do P.O.			

ANEXO 4

[Nome e sigla do projeto]
RESUMO DO SPRINT REVIEW – [Código do Sprint]

PARTICIPANTES	
Scrum Master:	
Product Owner:	
Scrum Team:	
Outros:	

OBJETIVO DO SPRINT

REQUISITOS SELECIONADOS			
# Ticket	**Título**	**Situação**	**Observação** (em relação a aprovação do cliente)
		Aprovado □ Sim □ Não	
		Aprovado □ Sim □ Não	
		Aprovado □ Sim □ Não	
		Aprovado □ Sim □ Não	
		Aprovado □ Sim □ Não	
Valores para Situação: "não implementado", "iniciado" ou "implementado".			

Data:	/ /	**Sprint:**	
Assinatura do P.O.			

ANEXO 5

Relatório de Acompanhamento de Projetos
[DIA] de [MÊS] de 2011

Sprint	2011.	**Data Início**		**Data Término**	
Projeto					
Gerente do Projeto [1]					
Gerente de Processos [2]					

[1] Ou representante do gerente do projeto.
[2] Ou representante do gerente de processos.

1 Atividades

1.1 O que deve ser divulgado?

- Reuniões com o cliente.
- Resultados já alcançados.
- Eventos
- Colocado em produção ou terminado a nível de funcionalidade

✓

1.2 O que foi feito?
- Anexar o relatório de Atividades do Redmine do Sprint atual

1.3 O que não foi terminado?
- Anexar o relatório de Atividades do Redmine do Sprint atual

1.4 O que vai ser feito?
- Anexar o relatório de Atividades do Redmine do próximo Sprint

2 Qualidade

2.1 A qualidade planejada está sendo seguida?

Avaliação de Qualidade	Está sendo satisfeita?	Observação

3 Acompanhamento de Problemas e Riscos

- Surgiu algum problema de hardware?
- Surgiu algum problema tecnológico?

3.1 Quais problemas surgiram?
- Anexar o relatório de Problemas abertos do Redmine agrupado por Sprint

3.2 Como estão os problemas antigos?
- Anexar o relatório de Problemas abertos do Redmine agrupado por Sprint

4 Avaliação da equipe
- Como está o desempenho de cada membro da equipe?
  - Alguma observação positiva?
  - Alguma observação negativa?

Membro	Papel	Observação	Comprometido*?
			□ Sim □Não

*Deve ser avaliado e confirmado o comprometimento de cada membro da equipe.

5 Avaliação do STI

- Existe alguma observação a ser feita sobre o STI?
  - O que está legal?
  - O que pode melhorar?
  - Alguma sugestão sobre o que poderia ser diferente para melhorar?

Bom	Pode melhorar
Sugestão	

6 Comprometimento

6.1 Clientes

Nome	Observação	Continua Comprometido
		□ Sim □ Não

7 Aderência ao Processo

7.1 Atualização dos documentos (MPS.BR)

7.1.1. Os **requisitos** estão atualizados no Plano do Projeto? □ Sim □ Não □ N/A
7.1.2. O **cronograma** está atualizado no Plano do Projeto? □ Sim □ Não □ N/A
7.1.3. Os **custos** estão atualizados no Plano do Projeto? □ Sim □ Não □ N/A
7.1.4. A **equipe** está atualizada no Plano do Projeto? □ Sim □ Não □ N/A

7.2 Reuniões

7.2.1 O Sprint Planning foi realizado? □Sim □ Não
Se Não, qual o motivo?

7.2.2 O Sprint Review foi realizado? □Sim □ Não
Se Não, qual o motivo?

7.2.3 A Sprint Retrospective foi realizada? □Sim □ Não
Se Não, qual o motivo?

7.2.4 As reuniões diárias estão sendo feitas? □Sim □ Não
Se Não, qual o motivo?

---

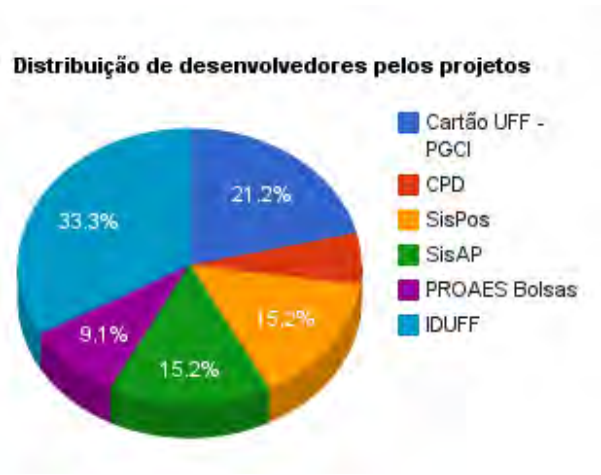
8 Comprometimento

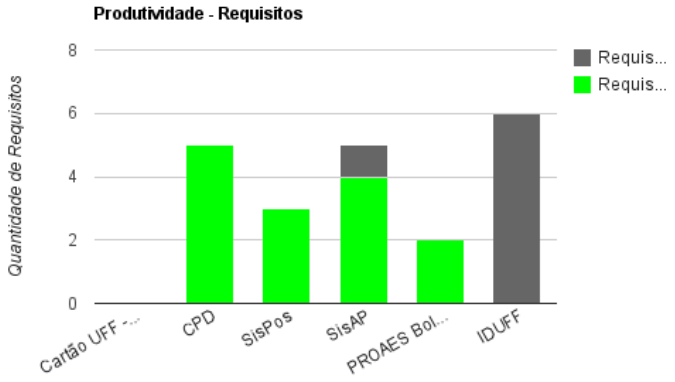
8.1.1 Todos os membros estão lançando horas? □ Sim □ Não
Se Não, qual o motivo?

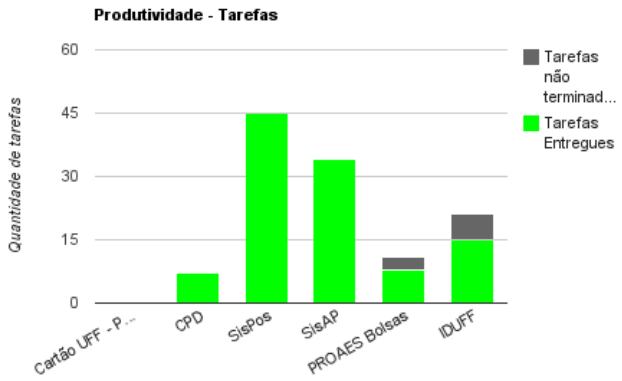
❖ Anexar o relatório de Horas do Redmine por dia de cada membro

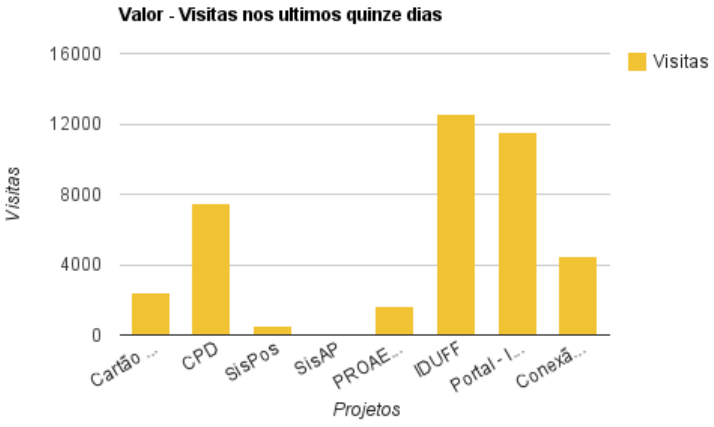
9 Observações
➢

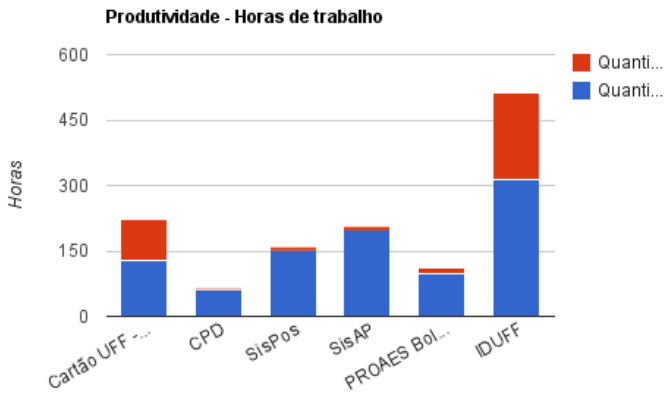
Painel de Acompanhamento de Projetos		
Preparado por:	[Nome da pessoa que preparou o documento]	Data: [data]
Sprint:		











UNIVERSIDADE FEDERAL FLUMINENSE – BOLETIM DE SERVIÇO
ANO XLI – N.° 050 31/03/2011 SEÇÃO II PÁG. 08

PORTARIA N.º 44.338 de 31 de março de 2011.

EMENTA: Reestruturação Administrativa, Relativa à Superintendência de Tecnologia da Informação.

O REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando a necessidade de dar continuidade à modernização da estrutura organizacional da Universidade Federal Fluminense;

RESOLVE:

I- **Ratificar** a criação da Superintendência de Tecnologia da Informação, vinculada ao Gabinete do Reitor, conforme determinado pela Decisão nº. 07/2010 e nº. 01/2011 através do desmembramento da estrutura da PROPLAN – Pró-Reitoria de Planejamento.

II- A Superintendência de Tecnologia da Informação - STI terá por finalidade básica realizar a gestão de infra-estrutura de software e hardware da Universidade, além de planejar e executar a política de informática da universidade. Também faz parte de sua missão pesquisar, desenvolver, executar e participar de projetos em Tecnologia de Informação e serviços de informática tanto internamente, nos diversos campi que compõe a UFF, como em parcerias com Municípios e Estados, além da captação de recursos através de projetos, consultoria e serviços em TI.

III- **Aprovar** a estrutura organizacional da Superintendência de Tecnologia da Informação, na forma dos Anexos I, II, III, respeitando-se o quantitativo de chefias estabelecido na Portaria Ministerial nº. 1.407 de 26/12/1996.

IV- Os órgãos que compõem a estrutura organizacional da STI, terão suas atribuições estabelecidas através do Regimento Geral da UFF.

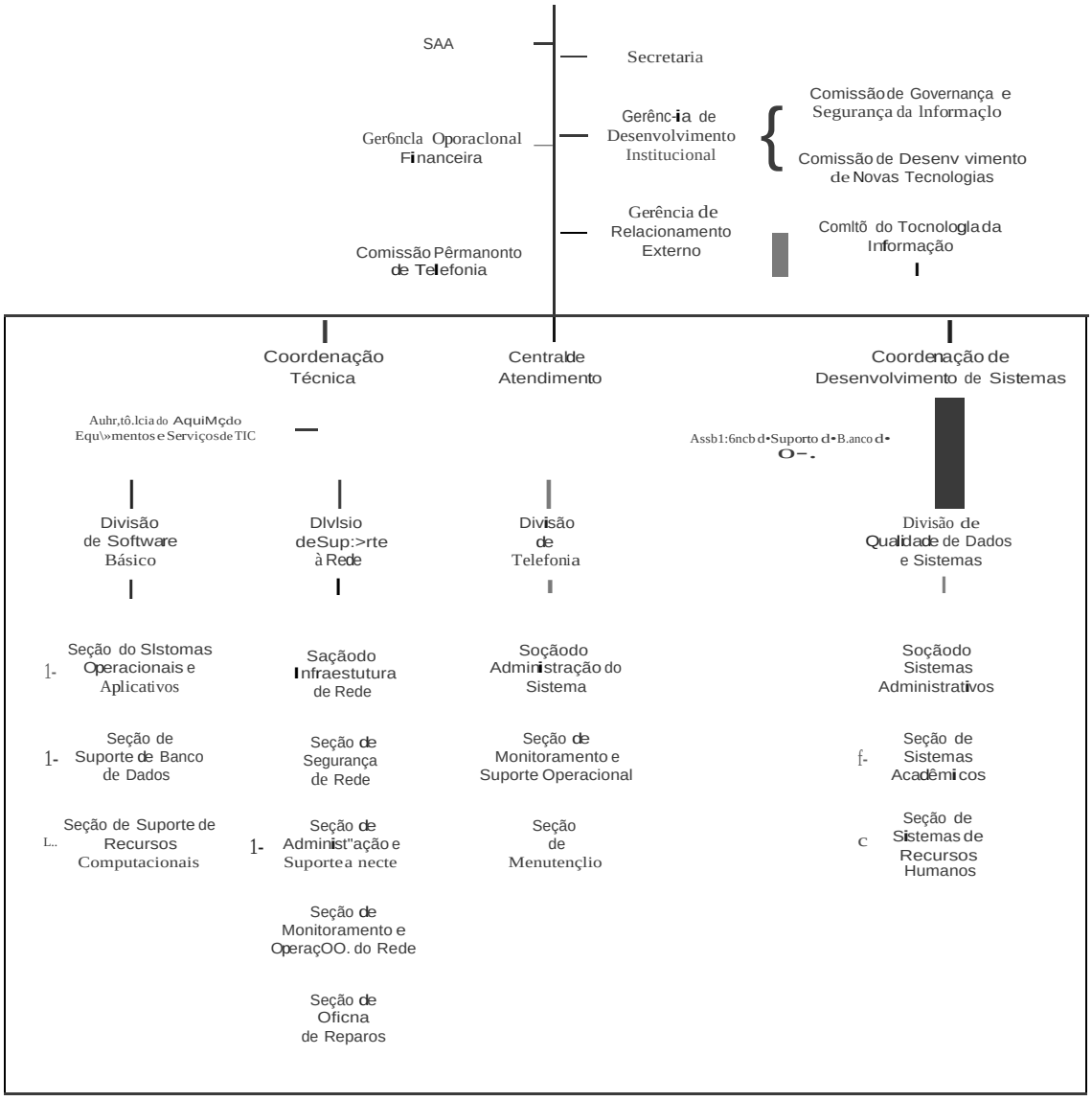
Publique-se, registre-se e cumpra-se.

SIDNEY LUIS DE MATOS MELLO
Vice-Reitor no Exercício da Reitoria
# # # # # #

Superintendência de Temologia da Informação- STI

ANEXOI

STI



Superintendência de Tecnologia da Informação - STI ANEXO II

QUADRO DEMONSTRATIVO DOS CARGOS EM COMISSÃO E DAS FUNÇÕES GRATIFICADAS DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO DA UFF VINCULADA A REITORIA

UNIDADE	**CARGO/ FUNÇÃO Nº**	**DENOMINAÇÃO CARGO/FUNÇÃO**	**CD/FG***
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO	1	Superintendente	CD-3
	1	Secretaria	FG-4
Setor de Apoio Administrativo	1	Chefe	FG-7
	2	Chefe	FG-4
	1	Chefe	FG-6
Gerência Operacional Financeira	1	Gerente	FG-1
Gerência de Desenvolvimento Institucional	1	Gerente	FG-1
Gerência de Relacionamento Externo	1	Gerente	FG-1
Coordenação Técnica	1	Coordenador	CD-4
Divisão	3	Chefe	FG-1
Seção	11	Chefe	FG-4
Coordenação de Desenvolvimento de Sistemas	1	Coordenador	CD-4
Divisão	1	Chefe	FG-1
Seção	3	Chefe	FG-4

* Dependendo da disponibilidade do cargo

Superintendência de Tecnologia da Informação - STI

ANEXO III – SIGLA DOS ÓRGÃOS NO SIORG-UFF

	SIGLAS
SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO	STI
SECRETARIA GERAL DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO	SA/STI
SERVIÇO DE APOIO ADMINISTRATIVO DA SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO	SAA/STI
GERÊNCIA OPERACIONAL FINANCEIRA	GOF/STI
GERÊNCIA DE DESENVOLVIMENTO INSTITUCIONAL	GDI/STI
COMISSÃO DE GOVERNANÇA E SEGURANÇA DA INFORMAÇÃO	CGSI/GDI
COMISSÃO DE DESENVOLVIMENTO DE NOVAS TECNOLOGIAS	CDNT/GDI
GERÊNCIA DE RELACIONAMENTO EXTERNO	GRE/STI
COMITÊ DE TECNOLOGIA DA INFORMAÇÃO	CTIN/GRE
COMISSÃO PERMANENTE DE TELEFONIA	CPT/STI
COORDENAÇÃO TÉCNICA	CTE/STI
ASSISTÊNCIA DE AQUISIÇÃO DE EQUIPAMENTOS E SERVIÇOS DE TIC	AES/CTE
DIVISÃO DE SOFTWARE BÁSICO	DSBA/CTE
SEÇÃO DE SISTEMAS OPERACIONAIS E APLICATIVOS	SSOA/DSBA
SEÇÃO DE SUPORTE DE BANCO DE DADOS	SSDB/DSBA
SEÇÃO DE SUPORTE DE RECURSOS COMPUTACIONAIS	SSRC/DSBA
DIVISÃO DE SUPORTE À REDE	DSRE/CTE
SEÇÃO DE INFRAESTRUTURA DE REDE	SIRE/DSRE
SEÇÃO DE SEGURANÇA DE REDE	SSRE/DSRE
SEÇÃO DE ADMINISTRAÇÃO E SUPORTE À REDE	SASR/DSRE
SEÇÃO DE MONITORAMENTO E OPERAÇÕES DE REDE	SMOR/DSRE
SEÇÃO DE OFICINA DE REPAROS	SORE/DSRE
DIVISÃO DE TELEFONIA	DTEL/CTE
SEÇÃO DE ADMINISTRAÇÃO DO SISTEMA	SASI/DTEL
SEÇÃO DE MONITORAMENTO E SUPORTE OPERACIONAL	SMSO/DTEL
SEÇÃO DE MANUTENÇÃO	SEMA/DTEL
CENTRAL DE ATENDIMENTO	CA/STI
COORDENAÇÃO DE DESENVOLVIMENTO DE SISTEMAS	CDS/STI
ASSISTÊNCIA DE BANCO DE DADOS	ABD/CDS
DIVISÃO DE QUALIDADE DE DADOS E SISTEMAS	DQDS/CDS
SEÇÃO DE SISTEMAS ADMINISTRATIVOS	SSAD/DQDS
SEÇÃO DE SISTEMAS ACADÊMICOS	SSAC/DQDS
SEÇÃO DE SISTEMAS DE RECURSOS HUMANOS	SSRH/DQDS

Demandas de serviços de TI da Comissão de Desenvolvimento de Novas Tecnologias

Projeto	Descrição	Cliente	Responsável	Valor que agrega à UFF	Status	Produtos e entregáveis	Estado atual	2011/2012
Suporte a infraestrutura de difusão de conteúdo multimídia	Implantar uma infraestrutura de difusão de conteúdo multimídia, para utilização em videoconferências, Webconferências e transmissões de eventos através da internet, além de prover suporte a outras necessidades	UFF	Hélcio	Melhoria no processo de comunicação da instituição	Planejado	1) Atualização do sistema de WEBTV 2) Implantação de um sistema centralizado de webconferência 3) Implantação de um sistema de TV nos restaurantes universitários	Iniciado	1) Atualização do sistema de WEBTV 2) Implantação de um sistema centralizado de webconferência 3) Implantação de um sistema de TV nos restaurantes universitários
Suporte à infraestrutura de EAD	Dar suporte a infraestrutura de serviços destinados a EAD, em especial ao software Moodle e soluções de hospedagem e divulgação de vídeos	UFF	Hélcio	Ampliação dos recursos de Ensino a distância	Planejado	1) Plataformas de EAD sob demanda 2)Plataformas multimídia sob demanda	Iniciado	1) Até 24 plataformas de EAD sob demanda 2) Até 12 plataformas multimídia sob demanda
Serviço de desenvolvimento de sites e portais	Atender às demandas da UFF no que se referir a desenvolvimento de sites e portais	UFF	Hélcio	Melhoria da divulgação dos projetos e demais atividades realizadas na Universidade	Planejado	1) Sites e portais sob demanda 2) Elementos gráficos e materiais de divulgação sob demanda	Iniciado	1) Até 180 sites e portais sob demanda 2) Até 24 elementos gráficos e materiais de divulgação sob demanda
Serviço de desenvolvimento de sistemas de apoio à gerência de serviços e à demandas específicas de usuários	Atender às demandas da UFF no que se referir a desenvolvimento de sistemas de pequeno porte	UFF	Hélcio	Propicia o uso mais adequado das plataformas de serviço disponíveis, bem como otimiza as atividades dos usuários com o uso de sistemas de TI	Planejado	1) Sistemas de pequeno porte sob demanda 2) Interfaces administrativas para serviços desenvolvidos pelo NTI sob demanda	Iniciado	1) Até 12 sistemas de pequeno porte sob demanda 2) Até 12 Interfaces administrativas para serviços desenvolvidos pelo NTI sob demanda

Portal NTI	Automatizar rotinas para solicitação de serviços ao NTI, através de seu portal, permitindo sua ativação automática	NTI	Hélcio	Melhoria na interface do NTI com a comunidade	Planejado	1) sistemas que possibilitem o acesso dos próprios usuários aos serviços fornecidos pelo NTI de forma automática 2) Desenvolvimento e implantação de sistemas para a administração dos serviços oferecidos pelo NTI, facilitando tanto os procedimentos dos administradores quanto os do suporte técnico	Planejado	1) sistemas que possibilitem o acesso dos próprios usuários aos serviços fornecidos pelo NTI de forma automática 2) Desenvolvimento e implantação de sistemas para a administração dos serviços oferecidos pelo NTI, facilitando tanto os procedimentos dos administradores quanto os do suporte técnico

Demandas de serviços de TI da Coordenação Técnica

Projeto	Descrição	Cliente	Necessidade atual	Valor que agrega à UFF	Status	Produtos entregáveis (próximos 12 meses)	Ao final de 2014	Vinculação ao PDI - UFF (2009-2012)
Suporte, manutenção e expansão da RedeUFF	Manter a atual e expandir a capacidade de acesso e disponibililidade da rede (cabeada e wireless), aumentando o desempenho da RedeUFF, proporcinando também maior mobilidade, em Niteroi e no interior do estado.	UFF		Aderência às metas do REUNI, no intuito de disponibilizar pontos de acesso para cada laboratório de pesquisa, áreas de convivencia, sala de professor, de aula e administrativa da Instituição, com desempenho compatível com as respectivas demandas.	Produção e evolução contínuada	1 - Capacidade de acesso aumentada em até 10% (900 novos pontos de acesso); 2 - Novos ambientes (predios, laboratorios etc.) conectadcos a RedeUFF; 2 - Aumento do desempenho e disponibilidade da rede	1 - Capacidade de acesso aumentada em até 25% (2.500 novos pontos de acesso); 2 - Desempenho adequado a futura demanda	**Área: Graduação e Pós-graduação** O1-E1-A3; O1-E1-A7 **Área: Pesquisa e Extensão** O1-E1-A7; O1-E2-A4; O2-E1-A6 **Área: Gestão de Pessoas** O1-E1-A1 **Área: Interiorização** O1-E2-A4; O2-E4-A7

Suporte, manutenção e ampliação nos niveis de segurança das informações eletronicas institucionais.	Manter os atuais niveis de segurança. Definir e implementar novos mecanismos que permitam obter melhorias consistentes na percepção interna e externa sobre a segurança no uso dos recursos computacionais providos pela RedeUFF	UFF		Constantes e consistentes melhorias na percepção interna e externa sobre a segurança no uso dos recursos computacionais providos pela RedeUFF	Produção e evolução contínuada	1 - Implementação de um novo modelo de segurança da RedeUFF, baseada nos padrões atuais; 2 - Rede e serviços mais seguros, estaveis e confiáveis.	1 - Manutenção do nível de segurança e confiabilidade alcançados; 2 - Adequação do modelo de segurança da RedeUFF, baseada nos padrões exigidos quando da ocasião.	**Área: Pesquisa e Extenção** O2-E3-A2 **Área: Planejamento e Gestão** O2-E1-A7; O2-E3-A2
Suporte e manutençao aos recursos computacionais e consultoria na aquisiçao de bens de TI	Manter e aprimorar a infraestrutura de hardware e software e oferecer assessoria técnica para aquisição de bens de TI (tangiveis e intangiveis)	UFF		Infraestrutura de hardware e software atualizadada e funcional, adequada as demandas locais de cada setor, servindo principalmente como ferramentas facilitadoras ao desenvolvimento das atividades institucionais.	Produção e evolução contínuada	1) Procedimento padrão de atendimento, registro e configuração/reparo de equipamentos 2) Modelo de gestão para aquisição de hardware e softwares 3) Otimização de serviços e custos com TI	1) Equipamentos atualizados/reparados em até 20 % do parque (2.000 computadores); 2) Critérios de aquisiçao padronizado; 3) Modelos para aquisição de hardware e software automatizados (via website)	**Área: Graduação e Pós-graduação** O1-E1-A3;O1-E1-A7 **Área: Pesquisa e Extensão** O1-E2-A7; O1-E2-A4; O2-E1-A6 **Área: Gestão de Pessoas** O1-E1-A1 **Área: Interiorização** O1-E2-A4; O4-E4-A3

Suporte à manutençao e implementaçao dos serviços de rede	Manter e aprimorar a oferta de serviços da RedeUFF, de acordo com a demanda da comunidade (WWW. Email, Portais, etc.)	UFF		infraestrutura de serviços de rede atualizadada, funcional, e atendendo as novas demandas	Produção contínua	Serviços de Rede com maior qualidade, disponibilidade, confiabilidade, e escalonável de acordo com necessidades dos usuários	1) Serviços atualizados de acoirdo com demanda	**Área: Graduação e Pós-graduação** O1-E1-A3; O1-E1-A7 **Área: Pesquisa e Extensão** O1-E1-A7; O1-E2-A4 **Área: Planejamento e Gestão** O2-E2-A1; O2-E2-A2 **Área: Interiorização** O4-E4-A9
Suporte à manutençao e implementaçao dos serviços de telefonia	Manter e aprimorar o sistema integrado de telefonia	UFF		Infraestrutura comunicação telefonica e atualizadada e funcional. Aderência às metas do REUNI, no intuito de disponibilizar pontos de acesso para cada laboratório de pesquisa, áreas de convivencia, sala de professor, de aula e administrativa da Instituição, com desempenho compatível com as respectivas demandas.	Produção contínua	Serviços de Telefonia (fixa e celular) com maior qualidade, disponibilidade, confiabilidade, e escalonável de acordo com necessidades dos usuários	1) Serviços atualizados de acordo com demanda 2) Ampliação da rede em até 10% (400 ramais fixos ou móveis)	**Área: Graduação e Pós-graduação** O1-E1-A7 **Área: Pesquisa e Extensão** O1-E1-A7; O1-E2-A4; O2-E1-A6 **Área: Interiorização** O2-E4-A8

Implementação de um mecanismos de autenticação de acesso à RedeUFF	Prover um mecanismos de autenticação de acesso à RedeUFF, cabeada e wireless	UFF		Autenticação centralizado e seguro, possivelmente integrado a outras instituições (projeto IC - Eduroam)	Planejamento	1) Estudo de viabilidade do acesso via sistema de diretórios 2) Implantação de gerência de distribuição de contas e senhas de acesso 3) Implantação do sistema de autenticação do acesso	1) Estudo de viabilidade do acesso via sistema de diretórios 2) Implantação de gerência de distribuição de contas e senhas de acesso para toda a comunidade universitária 3) Implantação do sistema de autenticação do acesso	**Área: Graduação e Pós-graduação** O1-E2-A1; O2-E1-A6 **Área: Pesquisa e Extensão** O2-E1-A1 **Área: Interiorização** **O2-E4-A7**
Implementaçao de um Sistema próprio de telefonia VoIP	Suporte técnico na Elaboração de um projeto para o desenvolvimento de um sistema próprio de telefonia VoIP (voz sobre IP) para UFF, objetivando a eliminação dos gastos atualmente despendidos com a locação de equipamentos e sistemas especializados	UFF		Otimizar gastos com o Sistema de Telefonia e adicionar novas facilidades	Planejamento	Projeto Piloto	1) Projeto piloto em processo de homologação 2) Definição / Aquisiçao de equipamentos para a 2ª etapa 3) teste inicio do processo de homologação da 2ª etapa) processo de homologação da 2ª etapa 5) Impantação e testes iniciais em localidades geograficamente distantes em paralelo com o sistema atual	**Área: Graduação e Pós-graduação** O1-E2-A1; O2-E1-A1 **Área: Pesquisa e Extensão** O2-E1-A1 **Área: Interiorização** O2-E4-A8

Demandas de serviços de TI da Coordenação de Desenvolvimento de Sistemas								
Projeto	Descrição	Cliente	Necessidade atual	Valor que agrega à UFF	Status	Produtos entregáveis (próximos 12 meses)	Ao final de 2014	Vinculação ao PDI - UFF (2009-2012)
Acadêmico da Graduação	Administração Acadêmica da Graduação (Módulos CAEG, DAE e Suporte)	PROGRAD	Administração realizada no Sistema SIAD, necessitando atender regras como o módulo da CAEG e inscrição online de alunos	Administrar e gerir os dados acadêmicos dos alunos e cursos de graduação da UFF, com eficiência e da forma mais simples possível	Produção / Evolução	1) Manutenção das atividades de coordenação durante o período de ajustes e das atividades do DAE e CAEG - 09/11 2) Manutenção da integralização automática para DAE, CAEG, Alunos e Coordenações - 11/11 3) Migração das funcionalidades ainda restantes no SIAD - 03/12 4) Manutenção dos relatórios e funcionalidades migradas do SIAD - 06/12	Sistema configurável a ponto de atender as diferentes demandas de cada curso da UFF, acompanhando assim o crescimento do número de cursos e alunos	**Área: Graduação e Pós-Graduação O1-E1-A6; O1-E1-A1; Área: Interiorização O2-E4-A6;**

	Módulo de Diplomas	PROGRAD	Administração realizada no Antigo Sistema de Diplomas, causando diversos problemas e impactando no dia-a-dia das atividades da PROGRAD	Administrar as formaturas e realizar a integralização automática dos alunos da graduação, resultando em diplomas gerados pelo próprio sistema	Desenvolvimento	1) Implementação e execução da Carga de Dados do Antigo Sistema de Diplomas da PROAC - 09/11 2) Últimas validações, testes e aceitação do usuário - 09/11 3) Desativação do sistema antigo e entrada em produção do novo sistema - 10/11 4) Manutenção do módulo de diplomas - 01/12	Assinatura Digital dos diplomas gerados, permitindo assim verificação online dos documentos impressos	**Área: Graduação e Pós-Graduação O1-E1-A5; O1-E1-A4; Área: Interiorização O2-E4-A6;**
	Módulo de Quadro de horários Graduação	PROGRAD	Atualmente os departamentos e coordenações administram as turmas no sistema, porém, por se tratar de uma informação vital para a administração acadêmica, é preciso gerar conhecimento com esses dados	Alunos de graduação, professores, departamentos e coordenações acessarem o quadro de horários antes, durante e depois da inscrição online, com informações atualizadas e integradas ao sistema IDUFF.	Produção / Manutenção	1) Manutenção do Módulo no período de ajustes - 08/11 2) Desenvolvimento das interfaces de somente consulta do Quadro de Horários - 10/11 3) Quadro de horários de 2012/1 - 12/11 4) Manutenção da criação do quadro de horários de 2012/1 - 01/12 5) Desenvolvimento dos WebServices de leitura dos dados do Quadro de horários para outros sistemas - 03/12 6) Evolução do cadastro de turmas para contemplar integração com SIORG e com localização geográfica das turmas - 05/12 7) Quadro de horários de 2012/2 - 06/12	Sistema totalmente integrado com SIORG e gerando conhecimento geo-referenciado, aumentando a eficiência da gestão das turmas, facilitando para os departamentos, coordenações e alunos	**Área: Graduação e Pós-Graduação O1-E1-A6; Área: Interiorização O2-E4-A6;**

	Módulo de Lançamento de Notas da Graduação	PROGRAD	Sistema permite que Departamentos, Coordenações e Docentes informem suas notas, armazenando todas as ações executadas para garantir a segurança.	Registrar as notas dos alunos da graduação, possibilitando a integralização automática para diplomação	Produção / Manutenção	1) Verificação e preparação do sistema - 11/11 2) Preparar processamentos pós-lançamento de notas e pré-inscrição - 11/11 3) Lançamento das notas de 2011/2 - 12/11 4) Manutenção das notas lançadas - 01/12 5) Desenvolvimento do lançamento de notas para o DAE direto no histórico e de lançamento de dispensas - 10/11 6) Homologação da funcionalidade de alteração do histórico - 11/11	Notas lançadas com uso de Certificação Digital dos professores, aumentando assim a segurança do processo	**Área: Graduação e Pós-Graduação** **O1-E1-A6;** **Área: Interiorização** **O2-E4-A6;**
	Relatórios Acadêmicos para o MEC	PROGRAD	Atuamente os relatórios são gerados da base de dados do SIAD	Informar ao MEC os números da UFF, que servirão para a composição da matriz orçamentária do MEC para o ano seguinte	Produção / Manutenção	1) Geração do CENSO - 04/12 2) Geração do PINGIFES - 05/12 3) Geração do ENADE - 08/12	Relatórios gerados automaticamente por uma ferramenta web, evitando erros e problemas envolvidos no processo	**Área: Graduação e Pós-Graduação** **O1-E1-A6;** **Área: Interiorização** **O2-E4-A6;**
	Módulo de Declarações online	PROGRAD	As declarações muitas vezes precisam ser assinadas pelos coordenadores por falta dessa normatização e pelo regulamento não contemplar esse item. O módulo de declarações precisa ser uma aplicação única, possibilitando assim a geração e validação de declarações mesmo em períodos de muitos acessos como durante a inscrição online, por exemplo	Possibilitar a geração de declarações online facilitando o dia-a-dia de alunos e coordenações de curso, desburocratizando o acesso à informações acadêmicas	Produção / Manutenção	1) Manutenção do módulo - 09/11 2) Implantação da assinatura do Pró-reitor nas declarações - 10/11 3) Formalização de uma regra no regulamento de graduação e como portaria da UFF - 12/11 4) Planejamento e modelagem de uma solução independente de declarações - 02/12	Sistema independente servindo como repositório para todos os outros sistemas da UFF, simulando um cartório eletrônico, inclusive assinando digitalmente as declarações	**Área: Graduação e Pós-Graduação** **O1-E1-A6;** **Área: Interiorização** **O2-E4-A6;**

	Módulo de Inscrição Online para Alunos	PROGRAD	Atuamente os alunos se candidatam pelo IDUFF e acompanham durante todo o processo. As melhorias deste ano serão no sentido de facilitar a comunicação com os coordenadores e planos de turmas para vestibulandos no fim do ano	Possibilitar aos alunos da graduação que façam sua inscrição de qualquer local do mundo, desburocratizando esse complexo processo nas coordenações	Produção / Manutenção	1) Processamentos das inscrições e início do período de ajustes - 08/11 2) Desenvolver o Plano de Turmas para a inscrição de vestibulandos - 11/11 3) Planejar a Migração da Aplicação de Inscrição online para Alunos para a plataforma Ruby on Rails - 02/12	Sistema robusto, rodando numa plataforma isolada (Ruby on Rails), usando ferramentas de cache para aumentar o desempenho e Interface fácil para os alunos com avisos por e-mail e SMS	**Área: Graduação e Pós-Graduação O1-E1-A6; Área: Interiorização O2-E4-A6;**

	Módulo de Inscrição Online para Coordenações	PROGRAD	As coordenações hoje usam o sistema mas ainda reclamam de eventuais problemas principalmente durante a inscrição presencial e falta de comunicação direta com a equipe responsável. Além disso a falta de relatórios durante os períodos de processamento das inscrições.	Facilitar a gestão do processo de inscrição online para os coordenadores, com acesso a informações e decisões sobre vagas e turmas	Produção / Manutenção	1) Reunião para planejamento das atividades e levantamento dos problemas de 2011/1 - 09/11 2) Verificação e acerto de eventuais problemas levantados (fazer os testes de regressão) - 09/11 3) Convocar a equipe de UX para padronização e melhoria da interface de uso do sistema - 11/11 4) Inscrição online - 01/12 5) Processamento e relatórios para a inscrição online e resultados - 03/12 6) Reunião para planejamento das atividades e levantamento dos problemas de 2012/1 - 04/12 7) Verificação e acerto de eventuais problemas levantados (fazer os testes de regressão) - 04/12 8) Desenvolvimento da funcionalidade de 'Plano de Turmas' de vestibulandos para 2012/2 - 03/12 9) Homologação da funcionalidade de 'Plano de Turmas' de vestibulandos para 2012/2 - 04/12	Sistema robusto e estável (com poucos problemas) e fácil de usar, padronizado em relação a código e a interface de usuário. Facilitação para geração de relatórios customizados para cada coordenação e administração da inscrição pela equipe de desenvolvimento realizada via painel administrativo da inscrição.	**Área: Graduação e Pós-Graduação O1-E1-A6; Área: Interiorização O2-E4-A6;**

	Módulo de Ajustes para Coordenações	PROGRAD	A primeira vez que o sistema esteve em produção foi em 2011/1 e foi bem recebido pelos coordenadores de curso porém gerando alguns problemas naturais para uma primeira versão.	Facilitar a gestão do processo de ajuste dos planos de estudos para os coordenadores, com acesso a informações e decisões sobre vagas, turmas e situação de alunos	Produção / Manutenção	1) Acompanhamento e manutenção do módulo em produção - 09/11 2) Correção de eventuais problemas em produção - 09/11 3) Relatórios finais para fechamento do ajuste - 10/11 4) Re-abertura do Módulo para ajustes de 2011/1 5) Análise e levantamento da funcionalidade de solicitação de trancamento de disciplina pelos alunos - 01/21 6) Desenvolvimento da funcionalidade de solicitação de trancamento de disciplina pelos alunos - 02/12 7) Homologação da funcionalidade de solicitação de trancamento - 03/12 8) Entrega da nova funcionalidade de solicitação de trancamento - 04/12	Sistema totalmente estável, com diversas funcionalidades inovadoras como: solicitação de trancamento e inclusão feito pelo próprio aluno, dentro do sistema, trancamento, reabertura de alunos e apontamento de prováveis formandos de forma automática.	**Área: Graduação e Pós-Graduação** **O1-E1-A6;** **Área: Interiorização** **O2-E4-A6;**

	Módulo de Admissão de Alunos	PROGRAD	Atualmente arquivos são trocados entre COSEAC e NTI para geração das matrículas dos vestibulandos e entre DAE e NTI para geração das matrículas do SISU, gerando diversas inconsistências na base de alunos. Além disso, durante o acolhimento estudantil/matrícula apenas a documentação apresentada é validada, não gerando qualquer registro para a gerência dos vestibulandos pelo DAE	Unificar os processos e vias de entrada de alunos (Vestibulandos, SISU, etc...) com o objetivo maior de acolher melhor o aluno no dia da matrícula, gerando inclusive número de matrícula, conta no IDUFF e UFFMail no acolhimento estudantil	Análise	1) Modelagem e arquitetura da solução(grupo de arquitetura) - 10/11 2) Desenvolvimento da solução - 12/11 3) Homologação e testes da solução - 12/11 4) Entrega do módulo para produção - 01/12	Módulo totalmente funcional gerando matrícula e contas associadas, inclusive com digitalização dos documentos entregues pelos alunos para futura verificação. O Sistema também deverá validar automaticamente se os candidatos possuem matrícula ativa em outras universidades do Rio de Janeiro com o objetivo de fazer uma validação inter-institucional	**Área: Graduação e Pós-Graduação O3-E2-A1; Área: Interiorização O2-E4-A6;**
Acadêmico da Pós-Graduação	Sistema de Gestão Acadêmica da Pós-Graduação	PROPPi	Atualmente a PROPPi utiliza o Sistema Acol para algumas funcionalidades e outras bases de dados auxiliares (Access) para gestão dos cursos da PROPPi	Possibilitar à PROPPi gerir com qualidade os cursos de pós-graduação da UFF, podendo inclusive informar dados ao MEC automaticamente	Desenvolvimento	1) Análise do Sistema ACOL para migração dos dados - 09/11 2) Migração dos dados do Sistema ACOL para o novo SIstema - 08/11 3) Desativação do Sistema ACOL - 10/11 4) Entrega do módulo de cadastramento de alunos e geração de carteirinhas pela PROPPi - 10/11 5) Entrega do módulo de acesso dos alunos da Pós-Graduação - 12/11 6) Entrega do Módulo Administrativo (cursos, localidades, disciplinas e manutenção de alunos) - 03/12	Todas as funcionalidades implementadas e integradas ao IDUFF e outros sistemas da PROPPi, inclusive com geração de relatórios para o MEC	**Área: Graduação e Pós-Graduação O4-E2-A3; Área: Interiorização O2-E1-A3;**

Sistema de Controle de Processos e Documentos	Iniciar o desenvolvimento de um novo sistema de controle de processos e documentos na UFF com utilização das tecnologias GED e BPMN	UFF	Atualmente os processos e documentos de comunicação interna tramitam sob a forma de papel, causando diversos problemas como atraso no recebimento de documentos e, eventualmente, o extravio do mesmo, prejudicando dessa forma a gestão institucional	Proporcionar redução do trâmite de papéis no âmbito da administração da UFF.	Planejamento	1) Assinatura do termo de coperação com o Tribunal de Justiça do Rio de Janeiro (detentora do SIGA-DOC, solução a ser implantada na UFF) - 12/11 2) Início dos testes e homologação da solução SIGA-DOC a critério de testes - 12/11 3) Definição da política de Certificados Digitais para os usuários do SIGA-DOC através de convênio com uma Autoridade Certificadora, ligada à ICP-BRASIL - 06/12 4) Implantação em ambiente de produção dos primeiros memorandos eletrônicos (projeto piloto) - 08/12 5) Análise, desenvolvimento e implantação de outros documentos (processos, ofícios, etc) - 10/12 6) Manutenção dos documentos eletrônicos - 12/12	Início de estudos de ferramentas GED e BPMN para o desenvolvimento dos primeiros fluxos de processos e documentos na UFF, através da digitalização de documentos do Departamento de Contabilidade e Finanças	**Área: Graduação e Pós-Graduação O1-E1-A2; Área: Planejamento e Gestão O2-E2-A1;**
Intgração de dados entre a UFF e bases de dados de sistemas governamentais	Desenvolvimento de rotinas automatizadas em JAVA, RAILS, e DELPHI para viabilizar troca de dados entre a UFF e órgãos do governo estadual e federal	UFF	Atualmente as bases de dados da UFF ainda não estão totalmente integradas às bases do Governo Federal, impedindo a sincronia de dados com a plataforma do MEC de forma automatizada	Melhor participação na dotação orçamentária do MEC	Produção e em evolução continuada	Comunicação através webservices e atualização de bases de dados governamentais realizada de forma automatizada e independente de ação humana.	Sistema totalmente integrado às bases de dados do Governo Federal, objetivando assim a automatização dos processos internos integrados com as bases do Governo, evitando retrabalho e agilizando os processos UFF	**Área: Graduação e Pós-Graduação O1-E1-A6;**

Sistema do Organograma (SIORG-UFF)	Atualização dos atributos de dados do SIORG-UFF por seus principais clientes, em atendimento às necessidades do REUNI.	PROPLAN	A ineficiência da informação gerencial acarreta problemas no processo de tomada de decisão pela gestão. Dessa forma a unificação das bases de dados do Organograma (SIAPE, SIORG-MP e SCDP) torna-se necessária	Administrar e gerir os dados dos dos órgãos que integram a estrutura osganizacional da UFF para melhoria do processo de tomada de decisão gerencial.	Produção e evolução	1) Atualização da estrutura acadêmica com as Unidades (área física, identificação de salas de aulas, laboratórios e endereços) 2) Implantação do histórico das alterações dos órgãos 3) Manutenções necessárias nos sistemas SIAPE, SIRH e PATRIMÔNIO.	1) Implantar as alterações nas estruturas acadêmica e administrativa da UFF. 2)Implantação total dos atributos da base de dados pelos principais operadores (PROPLAN, PROGEPE e PREUNI).	**Área: Planejamento e Gestão** **O1-E1-A4; O5-E3-A1;**
	Planejamento da integração dos sistemas corporativos da UFF, a partir da reestruturação administrativa.	PROPLAN	A redundância da informação do Organograma leva naturalmente a falhas de desatualização, acarretando diretamente problemas na informação que é gerada em outros Sistemas Adminsitrativos	Administrar e gerir os impactos da integração nos sistemas internos e externos, a partir da reestruturação administrativa.	Análise, desenvolvimento e evolução	1) Início da análise, levantamento e criação de Grupo de Trabalho SIORG-UFF. 2) Modelagem e arquitetura da solução (grupo de arquitetura). 3) Desenvolvimento da solução. 4) Homologação e testes da solução. 5) Entrega do módulo para produção.	1) Identificar necessidades de manutenções nas bases de dados do SIORG e sistemas internos. 2) Efetuar manutenções nos módulos do sistema para vianilizar a integração implantar a integração. 3) Implantação da integração do SIORG com os sistemas de recursos humanos, patrimônio e pós-graduação.	**Área: Planejamento e Gestão** **O1-E1-A4; O5-E3-A1;**

Portal IDUFF	Sistema de identificação única da Universidade Federal Fluminense	UFF	O Sistema já contempla a autenticação via SSO (baseado em cookies e tokens) porém ainda precisa evoluir para absorver algumas funcionalidades que estão no IDUFF mas que são do Portal	Unificar e automatizar o processo de identificação de usuários através de login(CPF) e senha únicos, facilitando a administração do controle de acesso dos sistemas da UFF, beneficiando diretamente o usuário final (alunos, professores, funcionários, técnicos, etc)	Produção / Manutenção	1) Acompanhamento, manutenção e atualização da listagem de sistemas do Portal - 10/11 2) Documentação de uso do Portal por outras aplicações - 10/11 3) Desenvolvimento da funcionalidade de atualização de dados cadastrais - 12/11 4) Análise e modelagem de um painel de administração do Portal com funcionalidades como: localizar identificação, alterar senha de identificação, verificar log dos acessos de identificação, cortar acesso, criar acesso, etc - 01/12 5) Homologação da funcionalidade de atualização de dados cadastrais - 01/12 6) Desenvolvimento do Painel Administrativo - 03/12 7) Homologação do Painel Administrativo - 04/12 8) Entrega do Painel Administrativo - 06/12	Todos os sistemas e soluções WEB integradas com o Portal, facilitando a gestão de identificação dos usuários. Portal também controlando a autorização às funcionalidades e serviços de outras aplicações, estando totalmente integrado com a base LDAP oficial da UFF e com a Federação UFF para acesso em outras instituições	**Área: Graduação e Pós-Graduação O1-E1-A6;**

Consulta Pública UFF	Sistema de Consultas aos Dados Públicos da UFF	UFF	Sistema totalmente independente, sendo alimentado apenas com os dados de Turmas, inscrições e dados de alunos (evasão, etc) da Graduação	Proporcionar acesso aos dados públicos (números e dados estruturais) de todos os sistemas da UFF em um lugar centralizado e atualizado de forma automatica, tornando o funcionamento da UFF mais transparente	Produção / Manutenção	1) Manutenção do Sistema em produção - 10/11 2) Análise de uma forma automática de carregamento dos dados para a consulta pública - 11/11 3) Estudo e busca por ferramentas de Data WareHouse capazes de atender à necessidade da UFF - 01/12	Sistema totalmente alimentado com todos os dados públicos de todos os sistemas, facilitando a geração de conhecimento utilizando um Data WareHouse para facilitar as consultas e mineração desses dados	**Área: Graduação e Pós-Graduação O1-E1-A6; Área: Planejamento e Gestão O1-E1-A8; O3-E2-A1;**
Sistema de Recursos Humanos	Desenvolvimento de um novo sistema de recursos humanos para a UFF, totalmente integrado ao SIORG-UFF, através da internet.	PROGEPE	Atualmente a UFF utiliza um sistema de gestão de Recursos Humanos que prioriza a Folha de Pagamento da UFF, em detrimento às funções de gestão de pessoas (dados pessoais, funcionais e profissionais)	Fomentar a qualidade de dados e informações dos recursos humanos da UFF sobre dados pessoais, funcionais e profissionais dos servidores com mapeamento de competências	Análise	1) Início da análise, levantamento e priorização de módulos em conjunto com a PROGEPE. 2) Modelagem e arquitetura da solução (grupo de arquitetura). 3) Desenvolvimento da solução. 4) Homologação e testes da solução.	1) Análise das necessidades de alterações do modelo de dados; 2) Análise dos módulos de posse; frequência; controle de chefias; controle de adicionais diversos; processo de folha de pagamento; viabilidades de desenvolvimento de web services para o SIAPE; 3) Desenvolvimento web dos módulos acima; 4) Desenvolvimento de módulo de consultas gerenciais e relatórios.	**Área: Gestão de pessoas O2-E1-A1; O2-E1-A3; O2-E2-A2;**
Sistema de Bolsas da PROAES	Sistema de Gestão das Bolsas Assistencias da UFF	PROAES	A falta de uma ferramenta efetiva de gestão das bolsas assistenciais prejudica a otimização dos recursos da PROAES/UFF	Proporcionar um melhor gerenciamento dessas bolsas evitando disperdício e maximizando o acesso a elas	Produção e evolução	1) Manutenção do módulo de inscrição - 12/11 2) Desenvolvimento de novas necessidades do cliente - 01/12 3) Novos relatórios de análise dos dados de bolsas - 02/12 4) Integração com Sistema de Transportes do Rio - RioCard - com o objetivo de evitar o crédito em dinheiro para os alunos contemplados - 03/12	Todas as bolsas assistenciais da UFF deverão ser geridas pelo Sistema de Bolsas evitando assim a necessidade de novos recadastramentos, minimizando a redundância e facilitando o acesso para os alunos	**Área: Graduação e Pós-Graduação O1-E2-A3; Área: Interiorização O1-E3-A3;**

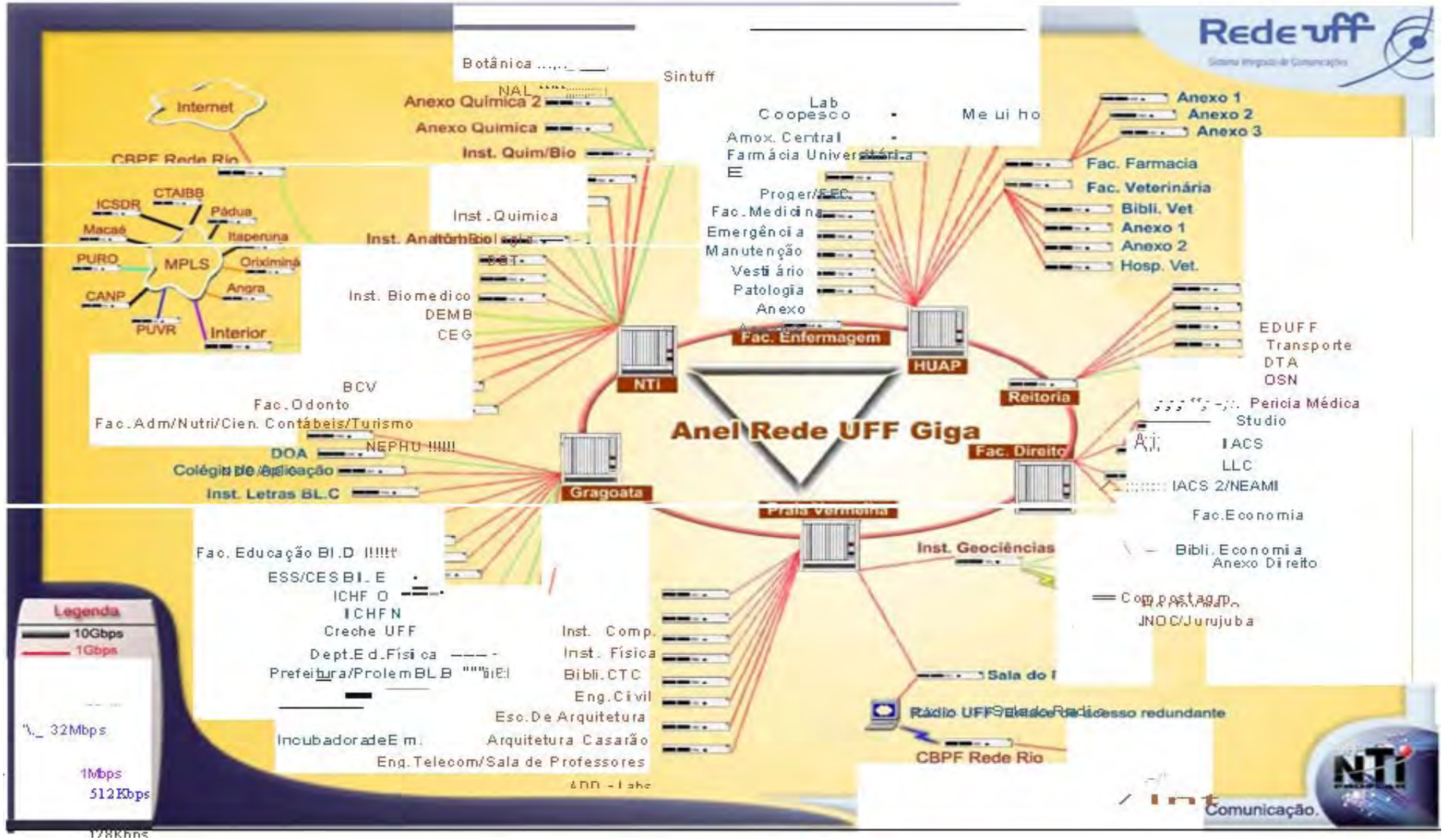
Cartão UFF	Solução de Cartões Inteligentes (SmartCards) para as pessoas da UFF	PROAES	A identificação de cada pessoa vinculada à UFF não é feita de uma forma unificada e segura, possibilitando fraudes em estabelecimentos e no próprio Restaurante Universitário da UFF	Proporcionar que cada pessoa na UFF tenha um Cartão Inteligente (SmartCard) com chip, possibilitando assim a identificação e autorização no controle de acesso a áreas seguras, aos restaurantes universitários, integração com transporte público e assinatura digital de processos críticos	Desenvolvimento	1) Início do uso de Totens de auto-atendimento, catracas, cancelas e portas seguras no Pólo de Volta Redonda - 11/11 2) Desenvolvimento do módulo de Controle de Transações Monetárias da UFF para atendimento aos Restaurantes Universitários da UFF - 12/11 3) Entrega do módulo de Controle de Transações Monetárias da UFF para atendimento aos Restaurantes Universitários da UFF - 01/12 4) Integração com Sistema de Transportes do Rio - RioCard - 01/12	Todos da UFF possuirão um Cartão Inteligente carregando seu certificado digital de identificação, podendo assinar documentos e e-mails, além de liberar acesso a diversas áreas e seguras, estacionamentos e laboratórios	**Área: Gestão de pessoas O1-E1-A2; O1-E1-A5; O1-E1-A6; Área: Planejamento e Gestão O1-E1-A5; O1-E1-A7;**
UFFMail	Solução de e-mail gratuito para alunos, professores e técnicos administrativos	PROGRAD	Solução de e-mail funcional para mais de 15.000 pessoas da UFF com mais de 2.500 acessos por dia, porém ainda com login não estando totalmente integrado com o Portal IDUFF	Proporcionar a todos que possuem um vínculo com a UFF de se comunicar com um e-mail institucional, válido para toda a vida	Produção / Manutenção	1) Acompanhamento dos acessos e eventuais problemas - 09/11 2) Análise da integração com o Login Automático do Google (SSO Google) para evitar a necessidade de fazer login para acessar o e-mail - 10/11 3) Desenvolvimento da integração com o SSO Google - 01/12 4) Entrega da integração com o SSO Google - 02/12 5) Análise da criação de Grupos(listas de e-mails) usando o UFFMail de forma automatizada e integrada com outros sistemas (ConexãoUFF, por exemplo) - 03/12	Demais serviços do Google já integrados aos sistemas da UFF, criando assim um ambiente de comunicação eficiente e eficaz entre todas as esferas da UFF	**Área: Planejamento e Gestão O3-E2-A4;**

Sistema de Administração Patrimonial	Desenvolvimento de um novo sistema de administração de bens patrimoniais com intgração total ao SIORG-UFF, através da internet.	PREUNI	Atualmente a UFF não conta com informações patrimoniais centralizadas e atualizadas em uma única base de dados, levando a instituição a não gerir de forma eficiente os recursos patrimoniais	Melhoria da qualidade das informações patrimoniais na UFF, com agregação ao sistema do patrimônio do HUAP, e controe de depreciação de bens móveis solicitados pelo governo federal.	Desenvolvimento	1) Principais cadastros do sistema desenvolvidos. 2) Modelagem e arquitetura da solução envolvendo carga de dados entre bases de dados ORACLE e MySQL (grupo de arquitetura). 3) Desenvolvimento do controle de bens ociosos. 4) Desenvolvimento de rotinas de depreciação diversas.	1) Análise do processo de importação de dados do sistema legado; 2) Análise do módulo de cadastro de bens patrimoniais; 3) Análise do módulo de controle de acesso e autenticação do sistema; 4) Análise do módulo de cadastro de fornecedores; 5) Análise do processo de imortação de dados do CONSIAFI; 6) Desenvolvimento dos módulos acima; 7) Desenvolvimento de módulo de consultas gerenciais e relatórios.	**Área: Gestão de pessoas O1-E1-A6; Área: Planejamento e Gestão O2-E1-A2; O2-E2-A7;**
Sistema de Monitoria	Sistema de Gestão das Bolsas de Monitoria da Graduação	PROGRAD	Sistema totalmente integrado ao IDUFF, porém ainda não integrado com o Login Único via Portal do IDUFF	Gerir de forma inteligente e automatizada o programa de bolsas de monitoria da PROGRAD, facilitando e desburocratizando o acesso às bolsas de monitoria e também a administração do processo como um todo	Produção / Manutenção	1) Manutenção do Sistema em Produção - 09/11 2) Análise da integração da Identificação de usuários através do mecanismo de SSO(Single Sign On) do Portal IDUFF - 10/11 3) Desenvolvimento da integração com o SSO do Portal IDUFF - 11/11 4) Entrega da integração com o SSO do Portal IDUFF - 02/12	Sistema totalmente integrado com outras plataformas/programas de Bolsas da UFF (como o PIBIC, e-fomento, etc) evitando assim que o aluno tenha mais bolsas do que é permitido. Além disso estará funcionando totalmente integrado com o Sistema Financeiro da UFF, facilitando a gestão de pagamentos	**Área: Interiorização O2-E1-A5; Área: Graduação e Pós-Graduação O1-E2-A3;**
PIBIC	Sistema de Gestão de Bolsas de Iniciação Científica da UFF	PROPPi	Sistema atendendo às necessidades da gerência de bolsas de iniciação científica da UFF porém com o método de acesso (login) não integrado ao Portal IDUFF	Gerir de forma inteligente e automatizada o programa de bolsas de Iniciação Científica da PROPPi, facilitando e desburocratizando o acesso às bolsas e a administração do processo como um todo	Produção / Manutenção	1) Manutenção do Sistema em Produção - 09/11 2) Análise da Integração com o SSO do Portal IDUFF - 10/11 3) Desenvolvimento da Integração com o SSO do Portal IDUFF - 12/11 4) Entrega da integração com o SSO do Portal IDUFF - 01/12 5) Manutenção do Sistema em Produção - 02/12	Evolução da solução e disponibilização como Software Livre para outras universidades	**Área: Graduação e Pós-Graduação O1-E2-A3;**

CPPD	Sistema de gestão dos concursos de docentes da UFF	CPD	Concursos realizados já usando o Sistema WEB do CPPD, porém ainda não integrado com RH/UFF	Otimização nos concursos de docentes, reduzindo atividades e etapas dispendiosas para a CPPD/UFF	Produção / Manutenção	1) Finalização do módulo de concursos - 09/11 2) Módulo financeiro - 10/11 3) Módulo de compra de passagem e hospedagem - 10/11 4) Cálculo de "Professores-Equivalentes" - 10/11 5) Módulo de pagamentos com GRU - 12/11 6) Internacionalização para inglês do sistema, junto com Feed RSS	Sistema de Seleção de professores totalmente integrado com o Sistema de RH da UFF, automatizando todo o fluxo de entrada de docentes. Disponibilização no Portal do Software Público Brasileiro - PSPB	**Área: Planejamento e Gestão O3-E1-A3;**
Implantação de SCRUM	As equipes de desenvolvimento devem ser treinadas para trabalhar com a metodologia ágil SCRUM.	STI	Foi realizado um Encontro Técnico sobre SCRUM com a maioria da equipe presente. Estão sendo planejadas novas ações e o treinamento constante dos times, necessário com a entrada de novos membros.	Aumento de produtividade das equipes de desenvolvimento e a qualidade dos produtos desenvolvidos	Desenvolvimento	Todas as equipes de desenvolvimento treinadas com SCRUM.	Envio de artigo para o Agil Brasil ou outro congresso de metodologia ágil mostrando um relatório técnico com nossa experiência com desenvolvimento ágil	**Objetivo estratégico da STI**
Implantação MPS.BR	Melhorar o processo de desenvolvimento de software, aumentando assim a qualidade do produto final produzido.	STI	Ja foi planejado o processo e as evidências para o nivel G do MPS.BR. Falta executar um projeto piloto com o processo planejado.	Um processo de desenvolvimento de software e uma avaliação MPS.BR nível G.	Desenvolvimento	Ter um projeto executado com o processo planejado.	Ter a avaliação MPS.BR nível G.	**Objetivo estratégico da STI**
Implantação da Central de Atendimento ao Usuário	Criar um canal de comunicação unificado do Usuário Final com as equipes de manutenção e suporte aos Sistemas	STI	Muitos atendimentos realizados porém com pouco acompanhamento gerencial e sem retorno (feedback) para as equipes de desenvolvimento	Melhorar o atendimento ao usuário final das soluções com o objetivo de fideliza-lo e propagar uma boa imagem para a comunidade da UFF	Produção / Evolução	Conseguir medir o impacto e a satisfação do cliente final	Centralizar todos os atendimentos de TI numa única central de atendimento com qualidade e padronização	**Objetivo estratégico da STI**
Implantação do Painel de Acompanhamento de Projetos	Criar um painel informativo e gerencial para o acompanhamento dos projetos de TI, com medições e resumo das métricas de cada projeto	STI	Criação do grupo de trabalho do PMO em andamento e conjunto de métricas já planejado	Facilitação na tomada de decisões e planejamento de novas ações sobre os projetos de TI	Produção e evolução	1) Acompanhar o preenchimento do painel - 10/11 2) Avaliar o uso do painel durante o ano e auxílio dos indicadores na tomada de decisões - 01/12	Disponibilizar uma TV de LCD em cada Pólo (NTI e NDC) de trabalho com o painel de acompanhamento dos projetos de TI	**Objetivo estratégico da STI**

Transferência de Tecnologia	Transferência de conhecimento tecnológico conforme determina a IN 04/2010 em seu artigo 14, inciso IV e alínea a	STI	Pouco investimento em desenvolvimento profissional dos servidores da área de Tecnologia da Informação	Melhoria da qualidade das soluções de TI produzidas, com conhecimento adquirido.	Produção e em evolução continuada	1) Transferência de conhecimento em tecnologias de desenvolvimento ágil (SCRUM, MPS.BR, REDMINE, e GESTÃO DE PROJETOS). 2) Armazenamento de dados dos sistemas corporativos; 3) Arquitetura para otimizar o fluxo de informações entre os sistemas.	Obter a melhoria da qualidade das soluções de TI para a comunidade acadêmica e definir indicadores de desempenho e qualidade das soluções. Divulgar, continuamente, os resultados na página da STI.	**Área: Gestão de pessoas O2-E1-A1;**
Sistema de Informações Gerenciais	Iniciar o desenvolvimento de um sistema de informações gerenciais para os principais gestores da UFF (GAR, PRÓ-REITORIAS, SUPER INTENDÊNCIAS, PÓLOS, e UNIDADES) e a sociedade.	UFF	A falta de informações precisas e atualizadas da gestão da Universidade sobre seus principais produtos, serviços e pessoas dificulta a tomada de decisão dos gestores da Instituição	Proporcionar informações para a melhoria da qualidade da tomada de decisão gerencial naUFF.	Análise	Estatísticas sobre cursos de graduação, pós-graduação, extensão e demais informações gerenciais aos principais gestores da UFF.	Apresentação de consultas e relatórios consolidados, com periodização identificada sobre totais relacionados às principais funções da UFF (produção, recursos humanos, contábeis, financeiras e de gestão) para os principais gestores da UFF.	**Área: Planejamento e gestão Objetivos: 2 Estratégias: 2 Ações: 2 Área: Interiorização Objetivo: 2 Estratégia: 4 Ação: 7**

ANEXO III


Rede uff
Internet
CBPF Rede Rio
ICSDR
CTAIBB
Pádua
Macaé
Itaperuna
PURO
MPLS
Oriximiná
CANP
Angra
PUVR
Interior
Botânica
NAL
Sintuff
Anexo Química 2
Anexo Química
Inst. Quim/Bio
Inst. Química
Inst. Biomedico
DEMB
CEG
BCV
Fac. Odonto
Fac. Adm/Nutri/Cien. Contábeis/Turismo
NEPHU !!!!!
DOA
Colégio de Aplicação
Inst. Letras BL.C
Fac. Educação Bl.D !!!!!
ESS/CES Bl. E
ICHF O
ICHF N
Creche UFF
Dept. Ed. Física
Prefeitura/Prolem BL.B
Inst. Comp.
Inst. Física
Bibli. CTC
Eng. Civil
Esc. De Arquitetura
Incubadora de Em.
Arquitetura Casarão
Eng. Telecom/Sala de Professores
Lab Coopesco
Amox. Central
Farmácia Universitária
Proger/EEC
Fac. Medicina
Emergência
Manutenção
Vestiário
Patologia
Anexo
Fac. Enfermagem
HUAP
NTI
Gragoata
Praia Vermelha
Reitoria
Anel Rede UFF Giga
Anexo 1
Anexo 2
Anexo 3
Fac. Farmacia
Fac. Veterinária
Bibli. Vet
Anexo 1
Anexo 2
Hosp. Vet.
EDUFF
Transporte
DTA
OSN
Perícia Médica
Studio
IACS
LLC
IACS 2/NEAMI
Fac. Direito
Fac. Economia
Bibli. Economia
Anexo Direito
Inst. Geociências
JNOC/Jurujuba
Sala do I
Rádio UFF
Acesso redundante
CBPF Rede Rio
Legenda
10Gbps
1Gbps
32Mbps
1Mbps
512Kbps
128Kbps
Comunicação.
NTI

PORTARIA N.º 47.106 de 13 de junho de 2012.

EMENTA: Aprova os termos contidos documento sobre Política de Segurança da Informação da Universidade Federal Fluminense (UFF) elaborado pelo Comitê de Tecnologia da Informação (COTI), instituído pela portaria nº 38.355, de 01.07.2008 e reformulado pela portaria n.º 44.709, de 23/05/2011. Este documento sobre a Política de Segurança da Informação faz parte integrante do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), aprovado pela portaria n.º 47.105, de 13 de junho de 2012.

O REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando o que determina o inciso VII do art. 5º IN GSI n.º 01, de 13 de junho de 2008 e observadas as diretrizes do Decreto n.º 3.505, de 13 de junho de 2000 e a Norma Técnica ABNT NBR ISSO/IEC 17.799: 2005;

Considerando esgotado o período de 11.01.2012 a 29.02.2012 relativo à consulta pública sobre Política de Segurança da Informação para coleta de críticas e sugestões dos principais gestores desta Universidade;

Considerando, ainda, a relevância dos trabalhos de publicação dos documentos emitidos pelo Reitor da Universidade Federal Fluminense,

RESOLVE:

1 - **Aprovar** os termos contidos nos documentos sobre **Política de Segurança da Informação** da Universidade Federal Fluminense, em anexo, elaborado pelo Comitê de Tecnologia da Informação (COTI), instituído pela portaria nº 38.355, de 01.07.2008 e reformulado pela portaria n.º 44.709, de 23 e maio de 2011.

2 - Este documento sobre a Política de Segurança da Informação da Universidade, faz parte integrante do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), aprovado pela portaria n.º 47.105, de 13 de junho de 2012.

Publique-se, registre-se e cumpra-se.

ROBERTO DE SOUZA SALLES
Reitor
# # # # # #

(ANEXO À PORTARIA N.º 47.106 de 13 de junho de 2012.)

EMENTA: Propõe os termos da Política de Segurança da Informação da Universidade Federal Fluminense.

A Política de Segurança da Informação da Universidade Federal Fluminense tem seus termos propostos, conforme segue:

Art.67. As questões relativas à Segurança da Informação, bem como, a administração e gestão da Segurança da Informação em Ambiente Computacional da Universidade Federal Fluminense ficarão única e exclusivamente a cargo da Área de Segurança da Informação da Superintendência de Tecnologia da Informação – STI da UFF.

Art.68. A Área de Segurança da Informação da STI será a responsável pela edição de Políticas, Normas e Procedimentos Institucionais que se façam necessárias para a garantia da Segurança e mitigação de riscos ao ambiente de Tecnologia da Informação – TI da UFF.

Art.69. A aprovação e promulgação de Normas e Procedimentos de Segurança da Informação Institucionais ficarão a cargo do Comitê de Tecnologia da Informação (COTI), enquanto para Políticas ficarão a cargo do Gabinete Reitor da UFF.

Art.70. Esta Política se aplica a todos os colaboradores da Universidade Federal Fluminense e seus órgãos, nos diversos níveis hierárquicos e vínculos – servidores, estagiários, trainees, temporários, fornecedores, clientes, terceirizados, etc – que a qualquer momento tenham necessidade de utilizarem os recursos de TI.

Art.71. Esta Política deverá obrigatoriamente sofrer revisões, no mínimo uma vez a cada ano-calendário, visando à garantia de manutenção da mesma atualizada, e condizente com as melhores práticas de Segurança, as novas ameaças, a evolução tecnológica da UFF, o crescimento da Instituição e suas constantes mudanças.

Art.72. A Área de Segurança da STI, juntamente com os Órgãos de Recursos Humanos, Jurídico da UFF e o Comitê de Tecnologia da Informação, deverá definir uma matriz de responsabilidades referente às aprovações e aos aprovadores no âmbito de TI, devendo, esse documento ser revisado no mínimo uma vez em cada ano-calendário. Essa matriz deverá obrigatoriamente contemplar os variados tipos e eventos de liberações de acesso e os respectivos responsáveis pela aprovação dos mesmos. Os usuários responsáveis deverão ser comunicados e estarem cientes que além da aprovação, poderão ser diretamente ou possuem corresponsabilidade acerca de eventos de mal-uso, descumprimento de normas ou ainda, infrações legais originadas de autorizações oferecidas pelos mesmos.

Art.73. Os processos, políticas, normas e procedimentos de Gestão de Riscos em Segurança da Informação deverão ser definidos pela Área de Segurança da Informação da STI e revisados periodicamente, no mínimo uma vez a cada ano-calendário.

Art.74. A Área de Segurança da Informação da STI será responsável pela edição e aplicação dos planos de Gerenciamento e Reposta a Incidentes, devendo os mesmos ser suportados por Política, Norma ou Procedimento específicos para tal, bem como, chancelados pelo Comitê de Tecnologia da Informação.

Capítulo I
Das Definições

Art.75. Para efeito dessa política considere-se:

V) **Ambiente Computacional:** é o conjunto de recursos computacionais separado para uma determinada função. Subdivido em:

V.I)**Produção:** ambiente que possui os dados reais do sistema, aquele que os usuários utilizam para as funções diárias e que cujas informações possuem valores legais e são aproveitadas pela instituição. Por possuir dados reais, é considerado ambiente extremamente crítico para a Segurança das Informações da Instituição e por isso, seu acesso deve ser limitado e somente liberado a quem realmente possui necessidade de utilizá-lo em tarefas do dia-a-dia e de alimentação de informações para o sistema.

V.II) **Homologação:** ambiente no qual são feitos os testes de um sistema e que um grupo restrito de usuários tem acesso para validação de funções de um novo sistema ou de novas funções para um sistema pré-existente. Possui cópias desatualizadas dos dados de produção. Por possuir dados reais, mesmo que desatualizados, possui razoável criticidade quando ao comprometimento da Segurança das Informações Institucionais.

V.III) **Desenvolvimento:** é o ambiente no qual os desenvolvedores de sistema possuem acesso para criar um novo sistema ou novas funções para um sistema pré-existente. Obrigatoriamente possui esquemas reais (tabelas, campos em tabelas) porém, preenchidos com dados falsos. Não compromete a Segurança das Informações da Instituição.

VI) **Perfil de acesso:** conjunto de regras de computação que liberam apenas determinadas operações em um sistema. É o perfil de acesso que determina as permissões de um usuário, ou seja, o que ele pode ou não fazer em um sistema.

VII) **Usuário Normativo:** usuário de área, ou seja, não é necessariamente um Analista de TI, que possui conhecimento profundo da área operacional e recebe conhecimento acerca dos perfis de usuário de um determinado sistema. É ele o responsável por aprovar a liberação de acesso de um determinado perfil de acesso a um determinado usuário. Ou seja, é ele o responsável por afirmar que as funções de um determinado usuário são compatíveis com o perfil a ser liberado para o mesmo.

VIII) **Área Normativa:** área da Instituição que é responsável pelas informações contidas em um sistema. O usuário normativo deve obrigatoriamente pertencer à Área Normativa.

Art.76. Compõem os recursos computacionais da UFF equipamentos integrantes de quaisquer ambientes computacionais supracitados, sejam estes de quaisquer tipos ou com quaisquer finalidades (computadores, notebooks, telefones, switches, hubs, impressoras, periféricos, etc.), independente de terem sido adquiridos pela instituição; uma vez integrantes de algum ambiente computacional, estão sujeitos a esta Política.

Capitulo II
Das Diretrizes Gerais

Art.77. A Segurança da Informação deve ser responsabilidade de todos, não apenas da área de TI. Desta forma, deve refletir em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso, solicitação de aprovação de recursos, etc.

Art.78. A Superintendência de Tecnologia da Informação irá providenciar os recursos humanos e materiais necessários para implementação das diretrizes estabelecidas nesta Política, bem como orientar

todos os usuários quanto as suas ações que serão tomadas, além de divulgar os preceitos de segurança da informação a serem observados por todos, inclusive, nas divisões, órgãos e campi da UFF que possuem ambiente de TI distinto, com maior ou menor integração com o restante da instituição;
Art.79. A utilização de informação e dos recursos computacionais deve ser sempre compatível com a ética, confidencialidade, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art.80. A utilização de recursos (sistemas, correio eletrônico, espaço em disco, equipamentos, etc.) disponibilizados pela instituição ou integrados ao ambiente desta (rede e afins), deve ser feita segundo os padrões e procedimentos definidos pela STI, visando manter a disponibilidade e o desempenho das aplicações.

Art.81. A conexão de equipamentos de terceiros na rede da instituição somente será permitida se não apresentarem risco ao ambiente corporativo e estiverem de acordo as políticas da instituição aplicáveis aos demais equipamentos, bem como, houver sido analisada e declarada adequada pela STI.

Art.82. As informações classificadas como confidencial e/ou reservada requerem alto grau de controle e proteção contra acessos não autorizados, como também, aquelas que necessitem de sigilo por força de lei ou contrato são candidatas naturais à obtenção dessa classificação. O direito de acesso a estas informações requer autorização expressa do Usuário Normativo e é regida por política específica de Classificação da Informação.

Art.83. A utilização indevida dos recursos computacionais pode provocar sanções a serem definidas pela STI e a Área de Segurança da Informação da STI, dentre elas a suspensão dos acessos, e deve ser notificada à Área de Segurança da Informação.

Art.84. Qualquer violação dessa política constitui base para uma medida disciplinar, inclusive o término do contrato empregatício, conforme Política Disciplinar, bem como, às sanções previstas por lei.

Capitulo III
Da Classificação das Informações

Art.85. A Classificação das Informações na UFF será regulamentada por política específica acompanhada de procedimentos específicos de manipulação, salvaguarda, transporte, criação e edição.
2.Toda informação criada no ambiente da UFF não classificada explicitamente será considerada informação Reservada

Capítulo IV
Da gestão da Segurança das Informações e suas responsabilidades

Art.86. A responsabilidade pela gestão da Segurança da Informação é atribuída aos agentes envolvidos no processo de criação, salvaguarda, transporte e destruição da informação, sendo assim caracterizados:

Normativos: responsáveis pela classificação da informação, pela definição de perfil do usuário e o tipo de acesso às informações;

Usuários: todos aqueles que utilizam os recursos de tecnologia da informação, sendo, portanto, responsáveis pelo conhecimento e aplicação dessa política;

Custodiante: responsável pela guarda da informação com segurança. Na UFF e nos seus campi, esse agente é a Área de Segurança da Informação da STI, que terá a incumbência de implementar e controlar as autorizações de acesso à rede, correio/e-mail, internet, sistemas, servidores, etc.; monitorar o uso adequado dos recursos liberados, bem como, de implementar e operacionalizar os mecanismos de segurança da informação.

Art.87. Os usuários normativos de natureza específica serão designados pelos 1º nível de reporte das áreas usuárias.
Art.88. Os gestores das Unidades Organizacionais da UFF são Usuários Normativos das informações pertencentes ao domínio de sua autoridade, e podem delegar as funções de concessão de direitos de acesso/homologação de alterações nos sistemas. Para tanto, devem formalizar estas delegações junto à Área de Segurança da Informação da STI.

Capitulo V
Da Segurança Física do Ambiente de TI

Art.89. Todos os equipamentos, incluindo suas movimentações, que compõem a estrutura do ambiente computacional da UFF, tais como servidores, roteadores, switches, hubs, controladores, impressoras, meios óticos e magnéticos de backup, computadores, etc., devem ser devidamente autorizados e registrados pela Divisão de Atendimento Técnico da STI.

Art.90. A UFF manterá dispositivos de proteção contra problemas de segurança física (condições ambientais adversas, desastres naturais, incêndios, etc.) e lógica (vírus, acesso não autorizado, invasões, etc.) compatíveis com os requisitos definidos nessa política. Cabe à STI a definição de tais dispositivos de proteção, considerando características regionais, a criticidade das informações e os recursos tecnológicos envolvidos. Nenhum fluxo de informações poderá existir sem que passe pelas camadas de proteção lógica.

Art.91. Para os sistemas classificados como de missão crítica, será utilizado hardware que disponha de recursos de redundância de processador, disco, energia, etc., bem como, equipamentos de prevenção e combate a incêndios (SPCI), além de controle da corrente elétrica (rede estabilizada), temperatura e umidade e acesso físico e lógico restrito.

Capitulo VI
Da Segurança Lógica do Ambiente de TI

Art.92. Cabe à Área de Segurança da Informação da STI garantir que todos os ambientes lógicos (sistemas operacionais, SGDBs e sistemas de informação) tenham o seu acesso restrito por senhas, estando em conformidade com as diretrizes descritas nessa Política, salvo em situações nas quais existam restrições técnicas impeditivas que serão analisadas pela área de segurança.

Art.93. Todo programa ou transação desenvolvido ou adquirido para execução no ambiente UFF deve, obrigatoriamente, conter as verificações de autorização de execução em perfeita sintonia com o ambiente tecnológico em que será processado. Não haverá exceção à verificação de autorização para execução de qualquer programa ou transação. A princípio, tudo que não for explicitamente permitido, está negado.

Art.94. Todo novo programa ou transação adquirido para execução no ambiente UFF deverá ser submetido à análise da Área de Segurança da STI afim de verificar sua conformidade.

Art.95. Nenhuma senha pessoal será gravada no código-fonte de programas, tampouco em arquivos ou tabelas destinadas a outros fins, devendo o tratamento desse tipo de informação seguir norma específica da STI para desenvolvimento e/ou aquisição de sistemas, softwares e afins.

Art.96. O acesso – mesmo que de simples consulta – aos arquivos ou tabelas de senha não será permitido, em nenhuma circunstância, a nenhum colaborador. Tal restrição será provida por mecanismos de segurança lógica ou criptografia;

Art.97. Toda conta de acesso sem uso há mais de 60 dias até o limite de 180 dias poderá ser desabilitada pela Área de Segurança da STI, sem prévia autorização do proprietário ou da Gerência para

isso, de modo a liberar recursos físicos e/ou licenças de softwares alocados. A exceção dessa regra é para usuários com primeiro nível de reporte à Reitoria, que serão contatados antes do recurso ser desabilitado;
Art.98. É proibida a desinstalação, nas estações usuárias, de softwares ou hardwares, que são utilizadas para realizar controle físico e lógico dos recursos disponíveis. Caso isso ocorra por procedimento indevido, o fato será comunicado, imediatamente, ao Superior Imediato e à Divisão de Atendimento Técnico, que apurará as causas, corrigirá o problema e providenciará a reinstalação;

Art.99. Somente será permitido o uso de recursos homologados e autorizados pela Instituição, desde que sejam identificados individualmente, inventariados, com documentação atualizada e atendendo a legislação pertinente em vigor. A utilização destes sem licenças correspondentes é crime, previsto na Lei 9.609, de 19 de Fevereiro de 1998. Portanto, qualquer usuário que exponha a Instituição a sansões jurídicas por utilização de softwares não homologados, independente de sua classificação (shareware, freeware, demo, etc.) sem respaldo das respectivas licenças, está sujeito às medidas disciplinares previstas, bem como, às sanções previstas por lei;

Art.100. A Homologação de recursos computacionais será de única e exclusiva responsabilidade da STI, sendo regida por norma e procedimento específico de Homologação de Software e Homologação de Hardware.

Art.101. Nenhum software, independente de suas condições comerciais, será instalado ou baixado para equipamentos UFF pelo próprio usuário, cabendo esta tarefa exclusivamente aos usuários alocados nas gerências e divisões da STI, que tem essa atividade inclusa no seu papel funcional. A exceção a essa regra somente poderá ocorrer mediante aprovação expressa da área de Segurança da STI, respeitando-se as premissas do item 4 dessa política. Tais liberações terão sempre efeito pontual e nunca serão vistas como permanentes e genéricas.

Art.102. A STI irá restringir as pessoas que poderão ser administradoras das respectivas estações de trabalho.

Art.103. No caso de contas de acesso standard e impossíveis de serem eliminadas ou alteradas, as senhas standard (que vem junto com o produto) serão, obrigatoriamente, modificadas imediatamente após a disponibilização do sistema e/ou ambiente, sem que haja solicitação específica sobre isso.

Art.104. É obrigatória e existência de planos de segurança e de infraestrutura para implantação de sistemas de informação, sendo que não serão implementados se trouxerem fragilidades que comprometam a segurança do ambiente UFF.

Capitulo VII
Do uso e formação das senhas

Art.105. Uma senha segura possui ao menos oito caracteres, inclui uma combinação de letras, números e símbolos e é fácil de ser lembrada, mas difícil de ser “quebrada”. Para a formação das senhas, serão adotados os seguintes critérios:

I)Tamanho mínimo de 8 caracteres.
II) Nunca podem ser nulas ou estar em branco.
III) Nunca visíveis na tela onde são informadas para atualização ou login.
IV) Nunca podem começar com os 3 caracteres iniciais do ID.
V) Mínimo de 2 dígitos numéricos.
VI) Mínimo de 2 caracteres alfanuméricos.
VII) Impedir a repetição de um mesmo caractere 3 vezes seguidamente.
VIII) Vetar a reutilização de ultimas 5 senhas utilizadas.
IX) Serem bloqueadas após 5 tentativas consecutivas e mal sucedidas de acesso.
X) Passar por rotinas de crítica que impeçam a utilização de senhas “fracas” ou “facilmente quebráveis”

XI) Evitar palavras dicionarizadas.

Art.106. Todas as senhas expirarão independentemente da vontade dos usuários, no máximo, a cada 45 dias. Além disso, todas as senhas iniciais – definidas pela Área de Segurança da Informação da STI quando da liberação do acesso – serão expiradas e, ao primeiro acesso de cada usuário, forçada a sua troca.

Art.107. As senhas pessoais podem ser trocadas pelo próprio usuário, independentemente da sua data de expiração. Porém, deverão ser impossibilitadas de serem trocadas mais de 1 vez no mesmo dia.

Art.108. Nenhum colaborador poderá usar de sua ascendência hierárquica ou funcional sobre outrem para determinar ou obrigar que este compartilhe sua senha pessoal de acesso com quem quer que seja. O usuário que porventura receba esse tipo de solicitação deve comunicar o fato à Área de Segurança da Informação da STI.

Art.109. O compartilhamento de senhas, individuais é proibido para todos os níveis da instituição. Da mesma forma, abrir uma conexão autenticada para deixar que outra pessoa a utilize. Em hipótese alguma, um usuário poderá passar sua senha pessoal de acesso para outrem. Tal ação, uma vez detectada, terá classificação de gravidade em função do ambiente em que ocorreu e será devidamente reportada aos superiores hierárquicos dos usuários e ao DDRH.

Art.110. Qualquer tentativa de “quebrar” (tentar descobrir) a senha pessoal de acesso de outra pessoal, ou mesmo invadir ambientes ou sistemas sujo acesso lhe é negado, serão notificadas aos superiores hierárquicos, e poderá resultar em medidas disciplinares apropriadas, conforme disposto na **Política Disciplinar**.

Art.111. É dever de todos, zelar pelo sigilo de suas senhas de autenticação, bem como escolher senhas fortes dificultando ser descoberta facilmente por outra pessoa.

Capitulo VIII
Da Segurança de Acessos

Art.112. A conta de acesso e a **senha** de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes à sua assinatura e representem nível de delegação concedida para o desempenho de suas funções.

Art.113. Os acessos externos a recursos da instituição (acesso remoto de colaboradores, terceiros, fornecedores, clientes, e outros casos que vierem a surgir) somente serão concedidos mediante autorização prévia, segundo instruções detalhadas caso a caso e realizadas por intermédio de soluções técnicas institucionais.

Art.114. O acesso à internet é permitido por intermédio de sistema de segurança institucionais. É proibido o acesso direto à internet por intermédio de provedores externos estando conectado à rede UFF.

Art.115. Eventuais interligações entre redes (de forma física e/ou lógica) envolvendo processo de automação e/ou informação somente deverão ocorrer utilizando soluções corporativas definidas pelo STI, de forma a garantir a disponibilidade, a integridade e a confidencialidade dos ambientes.

Capitulo IX
Do Controle de Acesso

Art.116. A Área de Segurança da Informação da STI deve assegurar que nenhum colaborador ou prestador de serviço obtenha direitos de acesso incompatíveis com a sua função, ou seja, cada usuário terá uma única conta de acesso por aplicação.

Art.117. A Área de Segurança da Informação definirá e adotará um padrão de identificação de usuários que permitirá associar, de maneira única, cada direito de acesso à pessoa que o detém e concederá direitos de acesso compatíveis com as funções desempenhadas pelos usuários, através de perfis de acesso diferenciados. Tais perfis objetivam restringir os dados e operações disponíveis, e sua definição será realizada em conjunto com Usuários Normativos.

Art.118. No caso de fiscais de outros órgãos públicos, mesmo não existindo vínculo direto, as pessoas também poderão ser cadastradas nos sistemas de RH, associados a um colaborados responsável e também controlados por data de vigência lógica.

Capitulo X
Da Segregação de Ambientes e Funções

Art.119. A STI deve assegurar que todos os sistemas de informação da Instituição sejam aderentes as diretrizes a seguir:

I) Segregação de ambientes lógicos, de maneira que o ambiente de produção fique apartado dos demais.

II) Os ambientes que não sejam de produção – ou seja, de teste, de homologação, de desenvolvimento e outros – devem ser de acesso exclusivo dos usuários envolvidos com atividades de desenvolvimento e suporte a sistemas. Estes usuários, nos ambientes de produção, podem efetuar, no máximo, operações de consulta.

III) O acesso às bases de dados dos ambientes de produção será feito, unicamente, através dos sistemas de informação, estando completamente vetado qualquer tipo de acesso direto. Os casos extremos de necessidade de liberação serão aprovados pela Área de Segurança da STI em conjunto com o usuário com nível gerencial da área solicitante.

IV) Todo objeto, tais como programas, telas, funções, etc., que for transferido para o ambiente de produção, deverá ser originado do ambiente de desenvolvimento ou de homologação, mantendo nesses ambientes o arquivo fonte original.

V) Deve existir nos ambientes de produção, sempre que tecnologicamente possível, um controle automático das versões dos programas-fonte. Este controle possibilitará a recuperação de versões recentes (dentro dos 6 meses predecessores e das 6 ultimas versões), assim como a identificação do responsável pela sua implantação. O acesso aos programas-fonte, principalmente de inclusão, exclusão e alteração nos seus códigos, será restrito, através de perfis de acesso específicos e registrado em trilhas de auditoria.

Capitulo XI
Do Plano de Contingência

Art.120. Para enfrentar situações de interrupção dos sistemas de informação, com consequente paralisação das atividades da UFF, a STI deverá manter um Plano de Contingência que permita operar os sistemas e recursos de forma que garanta um nível mínimo de operação.

Art.121. O Plano de Contingência deverá passar por revisões periódicas, no mínimo uma vez a cada ano-calendário.

Art.122. O Plano de Contingência deverá ser exercitado no mínimo 2 vezes ao ano.

Capitulo XII
Da Propriedade Intelectual

Art.123. Todos os sistemas, projetos e/ou configurações desenvolvidos para atender as necessidades e aos interesses da Instituição são de propriedade única e exclusiva da UFF, e somente poderão ser cedidos, comercializados ou distribuídos mediante a aprovação do STI. Essa regra deve ser formalizada em todos os contratos com fornecedores e prestadores de serviço ou atividades de desenvolvimento realizadas pela equipe de desenvolvimento UFF.

Art.124. A documentação dos sistemas de informação e projetos desenvolvidos, devem ser disponibilizadas em meio ótico ou magnético, contendo:

XII) Códigos fonte dos objetos (programas, telas, transações, etc.) desenvolvidos;

XIII) Manual do Usuário e/ou Help *On-Line*, desde que apresente explicações sobre funcionalidades e não apenas preenchimento de campos;

XIV) Diagrama de Contexto e Especificação Funcional;

XV) Diagrama de Casos de Uso e Casos de Uso;

XVI) Dicionário de Dados (DD);

XVII)Diagrama de Fluxo de Dados (DFD) ou Modelo de Transição de Dados (em projetos de automação, é indispensável os dois);

XVIII) Modelo de Entidade-Relacionamento (MER) ou Modelo de Objetos;

XIX) Diagrama de Classes

XX) E quaisquer outros artefatos de projeto e desenvolvimento gerados pela metodologia de projeto e desenvolvimento empregada no projeto.

Art.125. No caso dos sistemas de informação e automação desenvolvidos, implementados ou integrados por terceiros, a STI exigirá em contrato a disponibilização e atualização da documentação pertinente. Os pagamentos a serem efetuados ao fornecedor estarão condicionados à entrega de tal documentação, que poderá ser proporcional aos produtos entregues em cada fase do projeto.

Capitulo XIII
Da Auditoria e das Trilhas de Auditoria

Art.126. A Auditoria poderá ter acesso a qualquer informação que esteja armazenada em ambiente lógico (Sistemas Operacionais, SGDBs e Sistemas de Informação). Havendo evidência de qualquer atividade que possa comprometer a segurança do ambiente de TI, podendo a Auditoria auditar e monitorar as atividades de qualquer usuário, além de inspecionar seus arquivos e registros de acesso, sempre que julgar e comprovar necessidade.

Art.127. A STI deve providenciar os recursos tecnológicos para que as trilhas de auditoria sempre existam e fiquem disponíveis para uso, bem como definir o tempo de retenção e as informações que deverão sistematicamente e automaticamente compor os arquivos conhecidos como trilhas de auditoria.

Art.128. As trilhas de auditoria de um determinado sistema devem ser centralizadas evitando a sua dispersão em vários arquivos e ser de fácil acesso a quem de direito.

Art.129. As trilhas de auditoria devem registrar automaticamente todas as operações críticas efetuadas, e serão constituídas de, pelo menos, os seguintes campos: identificador do usuário (nominal, não podendo ser somente IP ou MAC Address), data da operação, horário da operação, operação realizada, dados antes da operação e dados após a operação.

Art.130. Sempre que surgir um novo ambiente lógico na instituição, a STI tomará a iniciativa de reunir-se com os Usuários Normativos correspondentes para deliberar sobre a criação das trilhas de auditoria.

Art.131. As trilhas de auditoria devem estar disponíveis para consulta por um prazo mínimo de 1 (um) ano, além de protegias contra inclusão, exclusão ou alteração de dados. As únicas inclusões de dados admissíveis serão as oriundas das rotinas automáticas de registro.

Capitulo IVX
Referências Normativas

Art.132. Este documento se ampara e referencia pelos instrumentos normativos apresentados conforme segue:

IX) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Publica Federal.

X) Decreto 4.553 de 27 de dezembro de 2002 – Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Publica Federal, e dá outras providências.

XI) Lei 9.609 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá providências.

XII) Instrução Normativa GSI/PR nº 01 de 01 de julho de 2008 – Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

XIII) Norma Complementar nº 03 de junho de 2009 à Instrução Normativa GSI/PR nº01 – Recomenda diretrizes para elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

XIV) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008.

XV) Portaria SLTI/MP nº05 de 14 de julho de 2005 – Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

XVI) ABNT NBR ISO/IEC 27001:2006 – Sistema de Gestão de Segurança da Informação.

IX) ABNT NBR ISO/IEC 27002:2005 – Código de Praticas para Gestão de Segurança da Informação.

PORTARIA N.º 47.107 de 13 de junho de 2012.

EMENTA: Aprova os termos da Norma de Aquisição de Recursos Computacionais da Universidade Federal Fluminense (UFF), elaborada pelo Comitê de Tecnologia da Informação (COTI), designado pela portaria n.º 44.709, de 23/05/2011. Esta Norma de Aquisição de Recursos Computacionais faz parte integrante do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), aprovado pela Portaria n.º 47.105, de 13 de junho de 2012.

O REITOR DA UNIVERSIDADE FEDERAL FLUMINENSE, no uso de suas atribuições legais, estatutárias e regimentais,

Considerando o que determina o inciso VII do art. 5º IN GSI n.º 01, de 13 de junho de 2008 e observadas as diretrizes do Decreto n.º 3.505, de 13 de junho de 2000 e a Norma Técnica ABNT NBR ISSO/IEC 17.799: 2005;

Considerando esgotado o período de 11.01.2012 a 29.02.2012 relativo à consulta pública sobre Norma de Aquisição de Recursos Computacionais para coleta de críticas e sugestões dos principais gestores desta Universidade;

Considerando, ainda, a relevância dos trabalhos de publicação dos documentos emitidos pelo Reitor da Universidade Federal Fluminense,

RESOLVE:

1 - **Aprovar os termos contidos na Norma de Aquisição de Recursos Computacionais,** elaborada pelo Comitê de Tecnologia da Informação (COTI), instituído pela Portaria n.º 38.355, de 01.07.2008 e reformulado pela Portaria n.º 44.709, de 23 e maio de 2011.

2 - Esta Norma de Aquisição de Recursos Computacionais da Universidade, faz parte integrante do Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), aprovado pela Portaria n.º 47.105, de junho de 2012.

Publique-se, registre-se e cumpra-se.

HEITOR LUIZ SOARES DE MOURA
Decano no Exercício da Reitoria
# # # # # #

(ANEXO À PORTARIA N.º 47.107 de 13 de junho de 2012.)

EMENTA: Propõe os termos da Norma de Aquisição de Recursos Computacionais da Universidade Federal Fluminense.

A Norma de Aquisição de Recursos Computacionais da Universidade Federal Fluminense tem seus termos propostos conforme segue:

Art. 17 - Quaisquer recursos que façam parte, se integrem, utilizem ou conectem ao ambiente de TI da Universidade Federal Fluminense devem exclusivamente seguir as normas de configuração, administração e controle da Superintendência de Tecnologia da Informação (STI).

Art. 18 - Recursos adquiridos mediante orçamento próprio dos órgãos constituem equipamentos da UFF e, portanto, serão administrados e controlados pela STI, devendo assim, estar de acordo com as normas e políticas desta.

Art. 19 - Recursos de propriedade particular de algum usuário necessitarão de autorização prévia e expressa da STI para que sejam conectados ao ambiente de TI da UFF. Neste caso, os mesmos também estão sujeitos às mesmas regulações que aqueles pertencentes à Instituição.

Art. 20 - Por ser parte do ambiente de TI da UFF, quaisquer recursos devem estar sujeitos a configurações por parte da STI, portanto, devem estar devidamente configurados para tal e adequados às normas da instituição.

Art. 21 - Os recursos e as informações presentes nos mesmos são de caráter institucional e estão sujeitos à monitoração por parte da STI, resguardados os garantidos pelas normas de classificação da informação e de acordo com o caso, a não divulgação dos responsáveis por parte da STI.

Capítulo I
Das Definições

Art. 22 - Para efeito dessa política considere-se:

I) **Órgão Avaliador:** é representado pela STI e tem responsabilidade de definir padrões e modelos de equipamentos, avaliar e homologar softwares, e possuir poder de veto a recursos que não estejam em concordância com o ambiente ou as normas da UFF.

II) **Usuário Solicitante:** é o usuário de qualquer área ou órgão da UFF, que identifica a necessidade e então inicia o processo de aquisição.

Capitulo II
Das Diretrizes Gerais

Art. 23 - A STI providenciará uma listagem contendo os softwares e outra os hardwares homologados para utilização no ambiente de TI da Instituição. As aquisições de soluções de TI devem obrigatoriamente priorizar os recursos constantes nestas listagens.

Art. 24 - A aquisição de recursos que não estejam presentes nas listagens de recursos homologados deverão obrigatoriamente possuir aprovação prévia da STI que verificará os seguintes itens:

I) Presença de similares em uso na Instituição, licenciados ou freewares/opensource, evitando duplicações de soluções similares e dispêndio desnecessário de recursos da instituição;
II) Adequação da solução apresentada ao ambiente de TI da Instituição, evitando incompatibilidades e possíveis falhas de segurança ou implementação;

III) Para os softwares licenciados, a existência de soluções adequadas ao usuário e opensource. Em adequação à Política de Segurança da Informação e às normas para TI na Administração Publica Federal – IN01 GSI/PR, ePing, Decreto 3.505, Lei 9.983.

Art. 25 - As soluções não presentes na listagem de homologados e aprovadas pela STI conforme Art. 2 desde documento serão catalogadas e inseridas na respectiva listagem.

Art. 26 - A STI deverá disponibilizar para consulta pública no âmbito da UFF as listagens de soluções homologadas.

Art. 27 - No caso de soluções não homologadas, a STI se responsabilizará por confeccionar o “padrão técnico” a ser anexado nos documentos de licitação.

Art. 28 - Todo o processo de homologação deverá ser documentado pelo prazo mínimo de cinco anos, incluindo documentos anexados, bem como, os “padrões técnicos” anexados às licitações.

Art. 29 - A STI esclarecerá por meio de seu serviço de HelpDesk o processo de homologação, assim como, quaisquer dúvidas relativas a aquisição de recursos computacionais.

Art. 30 - A aquisição de hardwares cujo uso destinar-se aplicações específicas que demandem software proprietário, comercial ou licenciado deve contemplar os referidos recursos. Por exemplo, a aquisição de um computador para uso de aplicações que demandem sistema operacional Windows, deve obrigatoriamente incluir nas especificações do computador a licença do sistema operacional em questão.

Capítulo II
Das penalidades e sanções

Art. 31 - A utilização de soluções não homologadas constitui infração à Política de Segurança da Informação, à Norma de Utilização de Recursos Computacionais e a diversas normas Federais, sendo, portanto passível de penalidades e sanções como as que seguem:

I) Indisponibilização em caráter temporário ou permanente do acesso ao recurso, não sendo necessário para tal prévio aviso por parte da STI.

II) Em caso de violação de patentes ou direitos autorias, a comunicação por parte da STI aos órgãos responsáveis, bem como, indicação do responsável ou responsáveis pela solução ou o ambiente no qual a mesma se encontre.

Capitulo III
Referências Normativas

Art. 32 - Este documento se ampara e referencia pelos instrumentos normativos apresentados conforme segue:

I) Decreto 3.505 de 13 de julho de 2000 – Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

II) Lei 9.983 de 14 de julho de 2000 – Altera o Decreto-Lei nº 2.848 de 7 de dezembro de 1940 – Código Penal e dá outras providências.

III) Norma Complementar nº 10 DSIC/GSIPR – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações, dos órgãos e entidades da Administração Pública Federal, direta e indireta.

IV) Norma Complementar nº 13 DSIC/GSIPR – Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

V) e-Ping – Padrões de Interoperabilidade do Governo Eletrônico, de 16 de dezembro de 2008

VI) Portaria SLTI/MP nº 05 de 14 de julho de 2005 – Institucionaliza os Padrões de Interoperabilidade do Governo Eletrônico – e-Ping.

VII) Lei 9.606 de 19 de fevereiro de 1998 – Dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no país e dá outras providências.