Universidade Federal do Rio Grande – FURG
Núcleo de Tecnologia da Informação

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

P S I

Versão : 1.0 – Novembro de 2012

ÍNDICE

1. Apresentação

Este documento estabelece a PSI - Política de Segurança da Informação da FURG, que é um conjunto das diretrizes necessárias à preservação e segurança dos bens de informação utilizados na Instituição.

São bens de informação :

- sistemas aplicativos desenvolvidos e adquiridos
- softwares básicos e de apoio
- dados
- hardware
- instalações físicas
- equipamentos de infra-estrutura
- documentos em papel

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegida.

A segurança da informação objetiva proteger a informação de diversos tipos de ameaças, para garantir a continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir em muitas formas :

- estar impressa ou escrita em papel
- armazenada eletronicamente
- transmitida através de meios eletrônicos
- em outros meios, imagens, filmes ou falada
- em conversas.

Seja qual for a forma de apresentação ou o meio através do qual a informação é apresentada ou armazenada, ela seja sempre protegida .

A segurança da informação é aqui caracterizada pela preservação da (ACID):

a) **Autenticidade,** que é a garantia de quem é o usuário real .

b) **Confidencialidade**, que é a garantia de que a informação é acessível somente a pessoas com acesso autorizado;

b) **Integridade**, que é a salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
c) **Disponibilidade**, que é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

A segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, instruções de trabalho e funções de software. Estes controles precisam ser implementados para garantir que os objetivos de segurança específicos da FURG sejam atendidos.

Os riscos típicos que a PSI da FURG pretende eliminar ou reduzir são:

a) Revelação de informações sensíveis;
b) Modificações indevidas de dados e programas;
c) Perda de dados e programas;
d) Destruição ou perda de recursos computacionais e instalações;
e) Interdições ou interrupções de serviços essenciais;
f) Roubo de propriedades.

2. Declaração de comprometimento da Administração Superior

A Administração Superior da FURG declara-se comprometida em proteger todos os ativos ligados à TI – Tecnologia da Informação garantindo a autenticidade, confidencialidade, a integridade e a disponibilidade de todos os ativos de informação.

3. As áreas de segurança da informação aqui tratadas são:

3.1. Segurança física

Conceituação – conjunto de medidas destinadas à proteção e integridade dos ativos da empresa e à continuidade dos seus serviços.
Vulnerabilidades – riscos naturais (inundações, tempestades etc.), riscos acidentais (incêndios, interrupções de abastecimentos etc.), entradas não autorizadas, roubos de patrimônio, etc.

Áreas sensíveis – instalações físicas, equipamentos, patrimônio físico, recursos humanos, etc.

3.2. Segurança lógica

Conceituação – conjunto de medidas destinadas à proteção de recursos computacionais contra utilização indevida ou desautorizada, intencional ou não.

Vulnerabilidades – acidentes por falhas (hardware, software, aplicativos e procedimentos).

Áreas sensíveis – sistemas operacionais, sistemas gerenciadores de banco de dados, sistemas gerenciadores de rede, sistemas aplicativos e ferramentas de apoio.

3.3. Segurança das comunicações

Conceituação – conjunto de medidas destinadas à proteção das informações que trafegam por meios eletrônicos ou convencionais e dos recursos utilizados para esse tráfego.

Vulnerabilidades – acessos não autorizados às redes de comunicação de dados, adulteração de dados em tráfego, utilização não autorizada de informações e extravio de formulários ou documentos classificados.

Áreas sensíveis – redes de comunicação de dados, redes locais, conexões com redes externas, ligações de usuários externos ao computador central.

3.4. Planos de continuidade

Conceituação – conjunto de planos que contemplam as atividades necessárias para a continuidade dos negócios, quando houver algum tipo de interrupção nos equipamentos críticos.

4. Diretrizes

Para o perfeito funcionamento da PSI da FURG, as seguintes diretrizes deverão ser implementadas e seguidas:

4.1. Aspectos organizacionais e administrativos

Sempre que necessário, para implementar e manter esta política, deverá ser utilizada consultoria especializada, com conhecimento nos diversos aspectos da segurança dos bens de informação e das tecnologias que os apóiam.

Convém que sejam estabelecidos contratos ou convênios para intercâmbio, contatos apropriados e consultoria permanente com

autoridades legais, sindicatos, organismos reguladores da área de segurança, organizações parceiras, fornecedores de serviços de uma forma geral, fornecedores de equipamentos e de infra-estrutura, fornecedores de software, fornecedores de serviços de telecomunicações, tendo como objetivo garantir ações eficazes e eficientes, quando da ocorrência de não conformidades de segurança.

A implementação da política deve ser feita de forma gradual, em função dos custos envolvidos e do impacto organizacional.

A responsabilidade por planejar a implementação da política ficará a cargo do CGI – Comitê de Gestor de Informática da FURG (criado por portaria do Gabinete do Reitor) e a execução das ações de segurança ficará a cargo do Grupo de Segurança da Informação do NTI.

4.1.1. Grupo de Segurança da Informação (GSI)

Deverá ser criado o GSI – Grupo de Segurança da Informação que terá a seguinte constituição: 1(um) representante da área de suporte, 1(um) representante da área de redes e 1(um) representante da área de sistemas de informação. O grupo será presidido pelo Diretor do NTI da FURG e, cada membro deverá indicar um substituto para seus impedimentos.

Principais atribuições do Grupo de Segurança da Informação:

a) Definir as normas, procedimentos e instruções de trabalho da PSI;
b) Definir as iniciativas para melhoria contínua das medidas de proteção dos bens de informação da FURG;
c) Encaminhar para analise e aprovação do CGI, normas e iniciativas de melhoria ou adequações de segurança da informação;

4.1.2. Termo de Responsabilidade (TR)

O Termo de Responsabilidade é o documento oficial da Universidade que compromete colaboradores, terceirizados e prestadores de serviço com a política de segurança da FURG. Este termo poderá ser implementado via documento formal(papel) e/ou de aceite de forma eletrônica, através dos sistemas.furg.br.

4.1.3. Atribuições e responsabilidades

Do ponto de vista da segurança da informação, são identificadas as seguintes funções genéricas, responsáveis pelo controle de acesso aos recursos da informação, com as respectivas atribuições e responsabilidades.

4.1.3.1. Proprietários das informações

São os diversos unidades, projetos e órgãos da administração da Universidade Federal do Rio Grande – FURG e para os quais a FURG presta serviços.

O proprietário da informação terá a autoridade e a responsabilidade de:

a) delegar responsabilidade e atribuições ao depositário das informações;
b) classificar os bens de informação, de acordo com sua natureza crítica e sigilosa;
c) estabelecer as regras de proteção dos bens de informação, quanto aos acessos, backups etc.;
d) monitorar o cumprimento das regras estabelecidas;
e) responder pelas violações registradas e participar da decisão a ser tomada, quando da ocorrência de não conformidade;
f) notificar não-conformidades de segurança.

4.1.3.2. Informações sobre custódia

O NTI-FURG é o responsável pelo processamento, armazenamento e custódia das informações e terá a responsabilidade de:

a) administrar os controles estabelecidos pelo proprietário da aplicação e de seus dados;
b) administrar o acesso aos recursos do sistema de processamento e prover procedimentos de segurança;
c) controlar o acesso à informação;
d) providenciar a proteção física;
e) simular e executar os planos de continuidade;
f) resolver as não-conformidades de segurança.

4.1.3.3. Usuário da informação

É todo servidor, discente, trabalhador temporário, estagiário ou terceirizados, que tenham acesso aos bens de informação da FURG.

O usuário da informação terá a responsabilidade de:

a) zelar por todo acesso ao ambiente computadorizado executado e registrado com a sua identificação de acesso;
b) respeitar e preservar o grau de confidencialidade da informação, divulgando-a exclusivamente para as pessoas autorizadas a terem esse conhecimento;
c) utilizar os recursos tecnológicos (equipamentos, programas e sistemas) e as informações somente para desempenho das suas atividades profissionais, sendo assim vedado o seu uso para fins pessoais;
d) assinar o TR - Termo de Responsabilidade onde são estabelecidas as regras sobre o uso dos bens de informação;
e) notificar não conformidades de segurança.

4.1.3.4. Chefia de Unidade

Servidor que ocupa cargo de gerência nas diversas áreas da Universidade.

A chefia de Unidade terá a responsabilidade de:

a) conhecer os procedimentos de segurança em vigência;
b) cuidar para que seus servidores estejam informados e cientes de suas responsabilidades em relação à segurança dos bens de informação;
c) implementar os procedimentos de segurança aprovados pela Instituição;
d) iniciar ação corretiva quando ocorram não conformidades ou quando sejam identificadas vulnerabilidades;
e) notificar não conformidades de segurança.

4.1.4. Classificação e controle dos ativos

Os ativos da FURG devem ser agrupados da seguinte maneira:

a) Os ativos de informação são os dados contidos em SGBD – Sistemas Gerenciadores de Bancos de Dados, os dados contidos em arquivos convencionais, a documentação de sistema – análise, usuário e operação – a documentação de softwares básicos e de apoio e os planos de continuidade;

b) Os ativos de software são os programas fonte, os jobs, as ferramentas de apoio ao desenvolvimento, os softwares básicos e de apoio e os utilitários;
c) Os ativos físicos são os equipamentos computacionais (computadores de grande porte, microcomputadores, notebooks, etc.), equipamentos de comunicação (controladoras, roteadores, modens, switchs, etc.), dispositivos de entrada e saída (discos, fitas, impressoras, etc.);
d) Os ativos de infra-estrutura são os no-breaks, os geradores de eletricidade alternativa, os quadros elétricos, os equipamentos de refrigeração, etc.

Para cada grupo de ativo, deverá ser feito um inventário contendo pelo menos as seguintes informações:

a) Ativos de informação: nome do ativo, responsável, usuário, localização, mídia;
b) Ativos de software: nome do ativo, fornecedor ou desenvolvedor, proprietário, localização, mídia;
c) Ativos físicos: nome do ativo, fornecedor, responsável, localização e capacidade;
d) Ativos de infra-estrutura: nome do ativo, fornecedor, responsável, localização e capacidade.

Para todos os grupos de ativos, também deverá ser feita uma classificação quanto à sua criticidade.

A classificação quanto à criticidade obedecerá aos seguintes critérios:

a) muito alta, quando a perda do ativo provocar parada total das atividades de TI;
b) alta, quando provocar perda parcial, de mais de 70% das atividades de TI;
c) média, quando provocar perda parcial, entre 30 e 70% das atividades de TI;
d) baixa, quando provocar perda parcial, abaixo de 30% das atividade de TI;
e) muito baixa, quando não provocar paradas na atividade de TI.

Particularmente para o ativo de informação deverá ser feita uma classificação adicional, quanto ao seu sigilo.

A classificação quanto ao sigilo obedecerá aos seguintes critérios:

a) confidenciais – informações para conhecimento de um grupo reduzido de usuários. Geralmente são informações de caráter pessoal;
b) restritas – informações de caráter setorial e para conhecimento de grupo reduzido de pessoas;
c) internas – informações pertencentes à FURG ou a órgão do Estado. Uma informação pode ser interna e restrita ou confidencial ao mesmo tempo;
d) públicas – informações que podem ser acessadas por qualquer usuário.

4.1.5. Recursos humanos

4.1.5.1. Recrutamento, seleção, admissão, transferência e demissão de pessoal ou encerramento de contrato

Serão adotados os seguintes procedimentos quanto para os do quadro temporário, terceirizados e prestadores de serviço:

a) obter referências pessoais e profissionais;
b) verificar a exatidão e inteireza do curriculum vitae, profissional e acadêmico;
c) checar a ficha policial, através da identidade;
d) providenciar a assinatura do TRS – Termo de Responsabilidade e Sigilo;
e) providenciar o ajuste do perfil de acesso aos sistemas, quando houver transferência de setor;
f) providenciar a eliminação do login, quando houver saída de pessoal, quer seja por demissão ou por suspensão de contrato;
g) na demissão do funcionário ou no encerramento de contrato, emitir um termo, isentando o usuário de responsabilidade sobre a utilização do login que está sendo eliminado, após seu desligamento.

Para o pessoal do quadro permanente valem as regras do serviço público federal.

4.1.5.2. Treinamento e conscientização

Será desenvolvido um programa de treinamento e conscientização dos usuários internos e externos, com as seguintes atividades:

a) planejar e executar seminários, de forma rotineira, tendo como objetivo a disseminação da cultura de segurança para os usuários dos serviços de TI ;

b) planejar, elaborar e distribuir, para todos os usuários, cartilha de segurança de bens de informação, abordando os aspectos fundamentais da mesma;

c) planejar, elaborar e solicitar alterações na página da FURG, para conter informações sobre segurança de bens de informação, tais como conceitos, definições, política de segurança etc.;

d) capacitar os profissionais que trabalharem no GSI, nas disciplinas de segurança;

4.1.6. Propriedade dos softwares aplicativos

Os sistemas aplicativos ou qualquer outro tipo de software, desenvolvidos ou adquiridos pela FURG, são de sua exclusiva propriedade e a sua utilização se restringe a apoiar os seus negócios.

4.1.7. Acesso à Internet, ao correio eletrônico

O acesso à Internet ficará restrito para as atividades profissionais e poderão ser utilizados mecanismos que monitorem e permitam o gerenciamento do uso desse recurso.

O endereço de correio eletrônico fornecido pela FURG para cada membro da comunidade universitária deve ser usado exclusivamente em suas atividades e poderão ser utilizados mecanismos que monitorem e permitam o gerenciamento da utilização do mesmo.

4.2. Segurança lógica

4.2.1. Gerenciamento das operações e comunicações

a) Documentação dos procedimentos de operação
Todos os sistemas, sejam eles executados em batch, on-line ou mistos, que estiverem em produção deverão estar com a documentação atualizada, conforme padrões da metodologia de desenvolvimento de sistemas em vigência no NTI-FURG.

b) Ambiente operacional
Todos os equipamentos de infra-estrutura, interligações das redes, interligações de hardware de grande porte e softwares

básicos e de apoio deverão manter uma documentação necessária e suficiente, que possibilite a qualquer técnico habilitado entendê-la, visando a manutenções preventivas, corretivas e evolutivas, no ambiente operacional.

c) Gerenciamento e controle de mudanças

Qualquer mudança no ambiente de produção, seja ela de infraestrutura, hardware, comunicações, softwares básicos, softwares de apoio, sistemas aplicativos, procedimentos etc., deverá ser planejada e documentada com no mínimo as seguintes informações:

- a descrição da mudança,
- os responsáveis por ela,
- a data e hora da execução,
- o tempo previsto,
- o impacto potencial
- um plano de recuperação em caso de insucesso

d) Gerenciamento e controle de problemas

Quaisquer problemas que ocorram no ambiente operacional, sejam eles de infra-estrutura, hardware, equipamentos de comunicação de dados, softwares e sistemas aplicativos, devem ser registrados com, no mínimo, as seguintes informações:

- a descrição do problema,
- a data e hora da ocorrência do mesmo,
- a identificação de quem o registrou
- de quem foi acionado para solucioná-lo,
- as conseqüências do problema,
- a data e a hora da solução,
- identificação de quem o solucionou
- a descrição da solução adotada.

e) Segregação de ambientes

Deverão existir três ambiente distintos de softwares, jobs, sistemas aplicativos, programas e dados:

- Ambiente de Produção

Conterá todo o ambiente de executáveis, em produção, dos sistemas aplicativos, jobs, softwares básicos, softwares de apoio e os dados reais residentes em arquivos convencionais e bancos de dados, necessários para a execução dos serviços da Instituição.

Este ambiente será de acesso exclusivo para aos servidores da Divisão de Suporte.

- Ambiente de Desenvolvimento – servidor de testes

Conterá todo o ambiente de executáveis, dos sistemas aplicativos, programas fonte, jobs de teste, softwares básicos, softwares de apoio e dados fictícios residentes em arquivos convencionais e bancos de dados, necessários para o cumprimento das tarefas da Divisão de Sistemas de Informação.

Em situações de exceção, servidores da Divisão de Suporte poderão acessar o ambiente de desenvolvimento, através de um login especial, que será criado com esta finalidade.

- Ambiente de Suporte

Conterá todo o ambiente de suporte: jobs de teste, fontes de softwares básicos, softwares de apoio e de sistemas aplicativos sob a responsabilidade da Divisão de Suporte , além de dados para testes, arquivos convencionais e bancos de dados.

Os aplicativos sob responsabilidade da Divisão de Suporte (fonte e executável de teste), os fontes e executáveis de softwares básicos e de apoio, no ambiente de suporte, serão executados pelos servidores da Divisão de Suporte autorizados para esta finalidade.

4.2.2. Planejamento dos recursos computacionais e aceitação de sistemas pela produção

a) Planejamento de capacidade

A atividade de planejamento de capacidade dos recursos computacionais deve ser contínua, tanto no ambiente de rede quanto no ambiente de equipamentos servidores. Devem ser apuradas, pelo menos uma vez por mês, a capacidade nominal, a capacidade efetiva e a carga atual dos recursos computacionais considerados críticos.

b) Aceitação de sistemas

Para serem aceitos no ambiente de produção, os sistemas aplicativos deverão estar previamente homologados pela Divisão de Suporte e documentados operacionalmente, conforme a metodologia de desenvolvimento vigente no NTI-FURG.

4.2.3. Procedimentos operacionais

a) Política de backups

Deverá ser estabelecida uma política de backups nas dependências da instalação principal e fora dela, que, em quaisquer situações permitam a recuperação de softwares, sistemas, dados, jobs e documentação, guardados em meio magnético.

Deverá ser simulada, periodicamente e por amostragem a recuperação destes backups.

b) Registros de operações

Deverá ser mantido um registro das operações de processamento, indicando quem executou o serviço, qual o serviço executado, a data e hora de início e fim e as ocorrências de não conformidades.

4.2.4. Segurança e tratamento de mídias

Para todas as mídias da Instituição que contenham bens de informação, sejam elas em meio magnético, ótico ou papel, deverão ser observados os seguintes cuidados:

a) Devem ser guardadas em lugar seguro e adequado à mídia, de acordo com as especificações do fabricante;

b) As que forem transitar para fora das instalações da FURG devem ter a sua saída registrada e a garantia de sua chegada ao destino. Além disso, devem ser embaladas de forma adequada, para garantir a sua integridade;

c) As mídias em meio magnético ou ótico devem ser identificadas externamente, quanto ao seu conteúdo, indicando, quando necessário, o prazo de retenção e observações sobre a mesma;

d) Quando forem descartadas, devem ser apagadas e/ou destruídas através de trituração ou incineração.

4.2.5. Controle de acesso aos recursos computacionais

a) Identificação e autenticação de usuários:

- O usuário somente tem acesso ao ambiente computadorizado através de uma identificação de acesso e uma senha;
- A identificação de acesso do usuário deve ser única, pessoal e intransferível;
- A senha associada à identificação de acesso deve ser secreta e de conhecimento exclusivo do usuário para o qual foi custodiada;
- A senha não pode ser divulgada a terceiros, devendo-se evitar o uso de combinação simples ou óbvia na sua criação;
- Não serão permitidas senhas para grupos de usuários;
- Quando o usuário errar a sua identificação ou sua senha, a mensagem emitida será sempre "Identificação/Senha incorretos";
- Sempre que possível e necessário, as identificações devem ser associados a uma determinada estação de trabalho;
- Sempre que possível e necessário, permitir identificação para apenas uma sessão, a cada acesso;

b) Regras para criação de identificações e senhas:

- Para servidores e alunos a identificação e senha são criadas no momento do cadastramento no sistemas da Universisdade, a identificação dos servidores é o número SIAPE e a senha no primeiro acesso é o CPF , a identificação dos alunos é o número de matrícula e a senha no primeiro acesso é data de nascimento . Os perfis iniciais são Professor para docente, Servidor para técnicos e Aluno para discente;
- Para outros que não servidores/alunos deverá ser encaminhado uma solicitação com os seguintes informações CPF, Nome e Data de Nascimento será criado um usuário cuja identificação será o CPF e a primeira senha o CPF , deverá constar quais os perfis de acesso que serão disponibilizados;

- Periodicamente, deve ser enviada para os proprietários da informação, uma relação dos servidores que tiveram seu identificação e perfil de acesso autorizados pelo mesmo. O proprietário deverá confirmar a informação, alterá-la indicando o novo perfil do funcionário ou revogar o identificação;
- A restauração de senhas é feita através do email ou de informações solicitadas do usuário. Não será permitida a restauração de senhas solicitadas por telefone;

c) Perfil de acesso dos usuários:

- Cada usuário terá um perfil de acesso, indicando os serviços;

- Sempre que necessário, deve ser estabelecido o mesmo perfil de acesso para um grupo de usuários.

4.2.6. Camadas de segurança

Para proteger o ambiente, deverão ser projetadas 4 camadas de acesso:

- ao ambiente,
- aos sistemas aplicativos,
- às funções dos sistemas aplicativos,
- aos dados.

Sempre que possível, a identificação e a senha deverão ser únicos para todas as camadas de segurança.

Deverão ser exibidos para os usuários apenas os arquivos, os softwares e as funcionalidades a que os mesmos têm direito de acesso.

4.2.7. Trilhas de auditoria

Os softwares de segurança deverão manter registros sobre os acessos dos usuários, indicando, sempre que possível, o arquivo, o software, a data e a hora que foram acessados.

Os SGBD – sistemas gerenciadores de bancos de dados deverão manter logs próprios que permitam a recuperação de informações.

4.2.8. Computação móvel e trabalho remoto

Trabalhos remotos devem ser evitados, ficando restritos aos servidores da FURG que tiverem esta necessidade. Para utilizá-lo deverá haver uma autorização prévia aprovada pelo Chefe da Divisão de Suporte. Para estes acessos, deverá ser considerada a possibilidade técnica e a necessidade de se estabelecer o mecanismo de rechamada (call back).

Sempre que necessário, a FURG disponibilizará sistemas na Internet. Para que estes acessos sejam feitos com segurança, deverão ser adotados mecanismos de proteção, tais como: certificação digital, softwares de segurança, antivírus, firewalls corporativos e individuais, criptografia etc., visando à proteção dos bens de informação.

Deverá ser planejada e implantada uma política que evite a execução de programas de origem duvidosa.

4.2.9. Trânsito de informações

Sempre que necessário e possível, as informações, tanto internas quanto externas, devem transitar criptografadas na rede.

4.2.10. Acesso a utilitários poderosos

A Divisão de Suporte deverá classificar todos os utilitários e programas considerados poderosos (tanto no ambiente de grande porte como nas redes locais) ou seja, programas que podem sobrepor os controles de segurança estabelecidos e implantados.

Esses utilitários, quando não puderem ser eliminados, deverão ter uma proteção de acesso, que os torne de uso restrito da Divisão de Suporte.

4.2.11. Administração dos acessos

Deverão ser criados mecanismos que permitam registros de acessos aos ambientes, indicando sempre que possível os recursos acessados, quem efetuou o acesso, data e hora, tentativas de acesso com senhas erradas, tentativas de acesso de estações de trabalho não permitidas, tentativas de acesso em horários não permitidos etc.

Deverão ser criados consultas e relatórios que permitam o monitoramento e gerenciamento dos acessos, pelas gerências imediatas, pela Divisão de Suporte e pelos auditores.

4.2.12. Desenvolvimento e manutenção de sistemas

O desenvolvimento de qualquer sistema, seja ele feito pela FURG ou por empresas terceirizadas, deverá utilizar na plenitude a metodologia padrão do ambiente vigente na FURG. Essa metodologia deve ser alterada, para contemplar os seguintes requisitos de segurança para os sistemas aplicativos:

a) Deverão ser criadas trilhas de auditoria, indicando quem acessou o mesmo e suas funções, a data, a hora, a identificação do registro modificado e a informação modificada;

b) Deverão ser criados arquivos de controle, com somatórios que permitam detectar e verificar qualquer irregularidade na entrada dos dados, no seu processamento e na saída dos mesmos;

c) Visando a recuperar informações, os aplicativos deverão guardar as movimentações, batch e on-line, que fizeram modificações nos seus cadastros. Se o SGBD suprir na plenitude esta função, o aplicativo não terá a obrigatoriedade desta guarda;

d) Os dados de entrada deverão ter rigidez na sua validação, tanto no nível sintático, quanto no semântico;

e) Quando necessário, deverá existir controle de sequência na execução dos programas;

f) Quando necessário, deverá existir controle de horário na execução dos programas;

g) Se necessário, algumas informações deverão ser criptografadas, quando forem guardadas.

4.3. Segurança física do ambiente

4.3.1. Áreas de segurança

Deverá ser estabelecido o perímetro físico do prédio do NTI-FURG, identificando todas as suas “fronteiras” e identificados todos os pontos de acesso.

Para as “fronteiras” com os prédios vizinhos, serão estabelecidos os controles necessários e suficientes, que salvaguardem o acesso às instalações do NTI-FURG. As entradas e saídas do prédio do NTI-FURG deverão ser dotadas da infra-estrutura necessária e suficiente que permita o controle adequado de entrada e saída.

4.3.2. Controles de entrada e saída de pessoas

a) Devem ser classificadas todas as áreas do prédio da FURG para acesso, quanto à criticidade
   - alta criticidade,
   - média criticidade,
   - baixa criticidade e
   - sem criticidade

   e quanto à restrição
   - alta restrição,
   - média restrição,
   - baixa restrição
   - sem restrição;

b) Devem ser criados mecanismos para identificação e controle de acesso de pessoas que não sejam servidores, às instalações do NTI-FURG, indicando quem teve acesso, data e hora e quem autorizou o acesso;

c) Os servidores terão seu controle de acesso através do registro de ponto eletrônico, que deverá ser disponibilizado nas portarias de acesso. Todos deverão registrar a entrada e saída, mesmo os liberados do controle de ponto. Apenas a diretoria estará dispensada do registro de entrada e saída;

d) Deverão ser criados mecanismos de acesso para servidores e não servidores, em horários especiais, fora do expediente normal, indicando quem teve acesso, data e hora e quem autorizou;

e) Devem ser criados mecanismos especiais que protejam o acesso aos locais considerados de alta restrição.

4.3.3. Proteção do prédio, equipamentos e da infra-estrutura

a) Os equipamentos, principalmente os considerados críticos, devem estar instalados em áreas protegidas de acesso;

b) Os equipamentos próprios, considerados de difícil reposição em função do custo financeiro, devem estar segurados, pelo menos contra incêndio;

c) As instalações prediais devem ser seguradas, pelo menos contra incêndio;

d) O cabeamento elétrico e de lógica, que alimenta e interliga os vários equipamentos, deve ser protegido de forma adequada;

e) Deverá ser instalado um sistema de no-break e um gerador de energia próprio, que alimentem pelo menos os equipamentos e os locais considerados críticos;

f) A manutenção preventiva dos equipamentos deve ser feita conforme as especificações do fabricante;

g) Devem ser criados mecanismos de proteção e combate a incêndio, principalmente em locais considerados críticos;

h) Deve ser criada e implantada uma brigada de incêndio;

i) Os procedimentos internos para proteção dos equipamentos devem ser replicados, sempre que possível e necessário, quando os mesmos forem deslocados para fora do NTI-FURG;

j) Devem ser planejados e implantados, onde for necessário, controles das condições ambientais.

4.3.4. Controles gerais

Deverá ser implantada a política de mesa e tela limpas, procurando evitar que documentos contendo informações confidenciais ou restritas fiquem expostos para pessoas não autorizadas, nas mesas ou nas telas das estações de trabalho.

Devem ser criados mecanismos para identificação e controle de qualquer movimentação, para fora do NTI-FURG, de ativos de TI, sejam

eles equipamentos, programas e dados contidos em mídias ou enviados via correio eletrônico, listagens contendo informações etc. Estas movimentações devem registrar quem as realizou, a data e a hora de saída e de retorno, quem autorizou e a identificação do ativo de TI movimentado.

4.4. Gestão de continuidade dos negócios

Visando garantir a continuidade dos negócios da FURG, devem ser preparados planos de continuidade. Deve existir, para cada situação, um plano de continuidade, contendo no mínimo as seguintes informações:

- objetivo do plano,
- análise de risco quanto à probabilidade e o impacto,
- condições mínimas de ativação,
- data de elaboração do plano, data de atualização do plano,
- data do último teste do plano e os resultados apresentados
- equipe que elaborou o plano,
- quais as pessoas que o executarão e seus substitutos imediatos
- cadeia sucessória de coordenação do plano
- os procedimentos para execução do mesmo.

Os planos de continuidade devem ser elaborados pelo GSI – Grupo de Segurança da Informação, com a colaboração da Divisão de Suporte e Desenvolvimento, apenas para os ativos considerados críticos. Eles devem ser aprovados pelo CGI.

4.4.1. Elaboração dos planos de continuidade

Devem ser planejados e elaborados planos de continuidade para no mínimo as seguintes situações de contingenciamento:

a) perda total do prédio;
b) perda de áreas críticas;
c) perda total dos processadores de grande porte;
d) perda de servidores de rede – arquivos, comunicação e aplicações;
e) perda de equipamentos de comunicação de dados (controladoras de comunicação, roteadores, switchs, modems, linhas, cabos etc.);
f) perda do sistema de I/O em disco;
g) perda de unidades de discos consideradas críticas;

h) perda do sistema de I/O em fita;
i) perda de impressoras consideradas críticas;
j) parada de softwares básicos (sistemas operacionais);
k) parada de softwares de apoio considerados críticos (sistema de comunicações de dados, sistemas gerenciadores de bancos de dados, etc.);
l) parada de aplicativos considerados críticos (sistemas de atendimento ao público, sistema financeiros, etc.);
m) greve de pessoal.

4.4.2. Validação dos planos de continuidade

Os planos de continuidade devem ser validados periodicamente, através de simulações. Os testes devem ser documentados e os planos corrigidos, quando se apresentarem insuficientes para recuperar uma situação real de contingência. As simulações terão a participação de todas as pessoas que foram definidas para a sua execução e serão coordenados pelo chefe do GSI.