FACULDADE SENAC – SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL
PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

JORGE ANTÔNIO COELHO DE SOUSA

ROBERTO RIVELINO DIAS

ROSSANO CANCELIER

SANDRO DOS SANTOS SOUZA

PLANO DE SEGURANÇA DA INFORMAÇÃO: DEPARTAMENTO DE ENG. QUÍMICA E ENG. DE ALIMENTOS - INSTITUIÇÃO DE ENSINO FEDERAL

FLORIANÓPOLIS, 2009

FACULDADE SENAC – SERVIÇO NACIONAL DE APRENDIZAGEM COMERCIAL
PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

JORGE ANTÔNIO COELHO DE SOUSA
ROBERTO RIVELINO DIAS
ROSSANO CANCELIER
SANDRO DOS SANTOS SOUZA

PLANO DE SEGURANÇA DA INFORMAÇÃO: DEPARTAMENTO DE ENG. QUÍMICA E ENG. DE ALIMENTOS - INSTITUIÇÃO DE ENSINO FEDERAL

Projeto Integrador de Curso de Pós-Graduação apresentado à banca examinadora da Faculdade Senac de Florianópolis como requisito parcial para a obtenção do título de Especialista em Segurança da Informação.

Orientador: Prof. Hélio A. Ferenhof, MBA, PMP

FLORIANÓPOLIS, 2009

JORGE ANTÔNIO COELHO DE SOUSA
ROBERTO RIVELINO DIAS
ROSSANO CANCELIER
SANDRO DOS SANTOS SOUZA

PLANO DE SEGURANÇA DA INFORMAÇÃO: DEPARTAMENTO DE ENG. QUÍMICA E ENG. DE ALIMENTOS - INSTITUIÇÃO DE ENSINO FEDERAL

Projeto Integrador de Curso de Pós-Graduação apresentado à banca examinadora da Faculdade Senac de Florianópolis como requisito parcial para a obtenção do título de Especialista em Segurança da Informação.

Aprovada em _____/_____/2009

_____

Aujor Tadeu C. Andrade

_____

Prof. José Mariano (Avaliador 1)

_____

Prof. xxxxxxx (Avaliador 2)

FLORIANÓPOLIS, 2009

Dedicatória

Dedicamos este trabalho às nossas esposas e filhos que sempre apóiam a nossa vida acadêmica.

AGRADECIMENTOS

Aos nossos pais, pelo carinho e apoio.
Aos nossos professores, pela dedicação na transmissão do conhecimento e incentivo à pesquisa.
Ao nosso orientador, Hélio Farenhof, pela atenção e competência.
À UFSC, por permitir a exploração do ambiente e possibilitar a conclusão deste trabalho.

RESUMO

A proteção e a preservação da informação são importantes em todas as áreas e numa instituição de ensino superior, que possui um departamento de pesquisa voltada para o desenvolvimento de patentes, não poderia ser diferente. O presente trabalho visa a elaboração de um plano estratégico de segurança da informação, baseado na norma NBR ISO/IEC 17799:2005, que proteja ou, no mínimo, diminua os riscos que estão expostos os ativos intelectuais desenvolvidos no Departamento de Engenharia Química e Engenharia de Alimentos da Universidade Federal de Santa Catarina. O desenvolvimento deste Projeto Integrador foi baseado em documentos de diversas fontes incluindo entrevistas e pesquisa de campo. Ao final do trabalho foram gerados documentos estratégicos que permitirão a tomada de decisão dos dirigentes do EQA no sentido de aumentar a segurança das informações geradas pelo Departamento. Apesar de abranger um escopo bem específico, fornece indicativos para o desenvolvimento de outros trabalhos semelhantes em outras áreas da Segurança da Informação.

Palavras chave: estratégia, informação, patentes, pesquisa, riscos, segurança.

ABSTRACT

The protection and preservation of information are important in all areas and at an institution of higher education, which has a research department focused on the development of patents, it could be different. The present study aims to develop a strategic plan for information security, based on standard ISO / IEC 17799:2005, to protect or at least lessen the risks faced by intellectual assets developed at the Department of Chemical and Engineering Food Federal University of Santa Catarina. The development of this project integrator was based on documents from various sources including interviews and field research. At the end of the working papers have been generated that will allow the decision of the leaders of the EQA to increase the security of information generated by the Department. Although covering a very specific scope, provides indicative figures for the development of other similar work in other areas of Information Security.

Keywords: strategy, information, patents, research, risk, security.

LISTA DE TABELAS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ANDES	Sindicato Nacional dos Docentes das Instituições de Ensino Superior
APUFSC	Associação dos Professores da Universidade Federal de Santa Catarina
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
CERTI	Fundação Centros de Referência em Tecnologia Inovadora
CESUSC	Complexo de Ensino Superior de Santa Catarina
CNPq	Conselho Nacional de Desenvolvimento Científico e Tecnológico
CONLUTAS	Coordenação Nacional de Lutas
COPERVE	Comissão Permanente do Vestibular
COPPE	Instituto Alberto Luiz Coimbra de pós-graduação e Pesquisa de Engenharia
CTC-UFSC	Centro Tecnológico da Universidade Federal de Santa Catarina
CUT	Central Única dos Trabalhadores
DIT	Departamento de Inovação Tecnológica
DRH	Departamento de Recursos Humanos
DSIC	Departamento de Segurança da Informação e Comunicações.
DSST	Divisão de Segurança e Saúde do Trabalhador
EMBRACO	Empresa Brasileira de Compressores
EQA	Engenharia Química e Engenharia de Alimentos
FAPESC	Fundação de Apoio à Pesquisa Científica e Tecnológica do Estado de Santa Catarina
FASUBRA	Federação dos Sindicatos dos Trabalhadores das Universidades Públicas Brasileiras
FATMA	Fundação do Meio Ambiente
FEESC	Fundação de Ensino e Engenharia de Santa Catarina
FEPESE	Fundação de Estudos e Pesquisas Sócio-Econômicos
FINEP	Financiadora de Estudos e Projetos

FUNJAB	Fundação José Arthur Boiteaux
GSIPR	Gabinete de Segurança Institucional da Presidência da República
IBAMA	Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis
IF-SC	Instituto Federal de Santa Catarina
MEC	Ministério da Educação
NDA	Núcleo de Desenvolvimento e Assessoramento Técnico
NIT	Núcleo de Inovação Tecnológica
NPD	Núcleo de Processamento de Dados
PETROBRAS	Petróleo Brasileiro S.A
PMF	Prefeitura Municipal de Florianópolis
RJU	Regime Jurídico Único
Sadia	Sadia S/A
SENAI	Serviço Nacional de Aprendizagem Industrial
SINTUFSC	Sindicato dos Trabalhadores da Universidade Federal de Santa Catarina
UDESC	Universidade do Estado de Santa Catarina
UFSC	Universidade Federal de Santa Catarina
UNISUL	Universidade do Sul de Santa Catarina
UNIVALI	Universidade do Vale do Itajaí

SUMÁRIO

1 INTRODUÇÃO

Sabe-se que em um ambiente acadêmico é comum que exista um grande fluxo de pessoas transitando pelos corredores dos diversos departamentos. Essas pessoas, em geral estudantes, misturam-se com funcionários, efetivos e terceirizados, gerando uma população de difícil controle e identificação.

Neste meio acadêmico, da mesma forma que existem pessoas bem-intencionadas, que buscam o aprimoramento intelectual ou desenvolver sua atividade profissional da melhor forma possível, também deve ser considerada a hipótese da presença de pessoas mal intencionadas e infiltradas na comunidade acadêmica, que visam à prática de atos ilícitos e antiéticos, provocando prejuízos à integridade moral e financeira da instituição.

Sabe-se também que na maioria dos estabelecimentos de ensino existe uma categoria de colaboradores responsável pelo zelo e controle do patrimônio, ou seja, dos ativos físicos. Mas, e quanto ao ativo não físico, intangível e que muitas vezes só é motivo de preocupação quando é perdido, extraviado ou danificado? Este é o caso da informação, que tanto pode ser de caráter acadêmico ou administrativo, mas que possui os mesmos riscos.

No ambiente de um departamento acadêmico existe uma gama de ativos tangíveis e intangíveis, que podem ser classificados como físicos, lógicos, patrimoniais, pesquisas, trabalhos acadêmicos, artigos, informação digital ou ativo intelectual, que necessitam de proteção e que serão objeto de estudo neste trabalho.

1.1 ESPECIFICAÇÃO DO PROBLEMA

Desde seu surgimento, o departamento de Engenharia Química e Engenharia de Alimentos (EQA), vêm acumulando informações administrativas e acadêmicas com regras amigáveis ou sem muito comprometimento com possíveis incidentes.

Vinculado ao Centro Tecnológico da Universidade Federal de Santa Catarina (CTC-UFSC), recebe diariamente uma grande quantidade de estudantes e pesquisadores que circulam por suas instalações para consulta e desenvolvimento acadêmico. Anualmente são desenvolvidas centenas de pesquisas acadêmicas que

são armazenadas na forma de mídia magnética e papel, que por sua vez, podem ser transformadas em um artigo, um registro de patente, um relatório técnico, uma publicação acadêmica (monografia, dissertação ou tese) ou outro tipo de publicação. Da mesma forma, existem informações administrativas, tais como orçamentos, normas ou documentos internos, que são gerados e mantidos pelos colaboradores do Departamento. Sem grandes preocupações, a entidade apresenta uma política ineficiente de contingenciamento e de segurança (física e lógica), desses ativos de informação.

Este Plano Estratégico em Segurança da Informação, utilizando-se de conceitos, metodologias e técnicas específicas, baseadas na NBR ISO/IEC 17799:2005 (ABNT, 2005) e na Cartilha de Segurança para Internet (CERT.br, 2006), se propõe a minimizar as principais vulnerabilidades existentes no Departamento em estudo.

1.2 OBJETIVOS

1.2.1 Objetivo Geral

Este trabalho tem como objetivo geral desenvolver o planejamento estratégico de segurança da informação, utilizando como cenário o Departamento de Engenharia Química e Engenharia de Alimentos da Universidade Federal de Santa Catarina, baseado na norma ABNT NBR ISO/IEC 17799:2005, visando proteger a área de pesquisa contra incidentes que comprometam os ativos intelectuais e administrativos.

1.2.2 Objetivos Específicos

- Definir proteções contra possíveis ataques cibernéticos à rede;
- Elaborar controle de acesso a conteúdos e seu manuseio;
- Elaborar solução para melhorar o índice de disponibilidade dos recursos computacionais;
- Elaborar o Plano de Continuidade de Negócio;

- Elaborar a Política de Segurança da Informação;
- Elaborar o Plano de Contingência.

1.3 JUSTIFICATIVA

Uma política de segurança é um instrumento para proteger a organização contra ameaças à segurança da informação que a ela pertence ou que esteja sob sua responsabilidade. Ela é compreendida neste contexto com a quebra de uma ou mais das suas três propriedades fundamentais:

> Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;
> Integridade: salvaguarda da exatidão e completeza da informação e métodos de processamento;
> Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. (FERREIRA, 2003)

1.4 FUNDAMENTAÇÃO TEÓRICA

O desenvolvimento da informática, também conhecido como “revolução digital”, através do progresso e difusão maciça dos microcomputadores, provocou mudanças radicais no modo de vida das pessoas e na forma das empresas realizarem seus negócios. Para ambos a informação instigou o aumento do conhecimento e a tomada de decisões estratégicas. A informação surge neste cenário como elemento principal da Era da Informação, onde “deparamo-nos com uma carga de informação cada vez maior” (SILVA FILHO, 2001) e que, devido à sua importância, necessita de proteção constante. Para minimizar os problemas de segurança foram desenvolvidas normas, políticas e também sistemas com o objetivo de fortalecer a segurança da informação contra os diversos incidentes do mundo virtual.

1.4.1 A Norma ABNT NBR ISO/IEC 17799

A Associação Brasileira de Normas Técnicas (ABNT), que é a responsável pelo Fórum Nacional de Normalização, em abril de 2001, disponibilizou para consulta pública o Projeto 21:204.01-010, que daria origem à norma nacional de segurança da informação: NBR ISO/IEC 17799:2001.

A versão final da NBR ISO/IEC-17799:2001, que é uma tradução literal da norma Internacional de Segurança da Informação - ISO/IEC-17799:2000, foi homologada em setembro de 2001 e sua publicação incluiu oficialmente o Brasil no conjunto de países que adotam e apóiam o uso da norma de segurança da informação (GONÇALVES, 2004). Em 30 de setembro de 2005, passou a ter validade a segunda edição atualizada da norma brasileira. Foi publicada sob o número ABNT NBR ISO/IEC 17799:2005, que é equivalente à norma ISO/IEC 17799:2005, entrando em vigor a partir de novembro de 2005 (MICROSOFT, 2006).

Esta versão da ISO/IEC 17799 vem sendo utilizada por vários países, como é o caso de Portugal, Angola e outros. Assim como a versão original, a norma brasileira de segurança de informação é dividida nos 11 macros controles:

- **Política de segurança da informação:** revisão e avaliação da política de segurança corporativa;
- **Organizando a segurança da informação:** estruturação interna da segurança, sobre o acesso de terceiros e terceirização de serviços;
- **Gestão de ativos:** contabilidade e inventário dos ativos e classificação das informações;
- **Segurança em recursos humanos:** segurança na definição das atividades a serem executadas e no recrutamento de pessoal, treinamento em segurança e na execução das funções atribuídas;
- **Segurança física e do ambiente:** definição das áreas seguras, segurança dos equipamentos e controles gerais (política de mesas e telas limpas, remoção de ativos, etc.);
- **Gerenciamento de operações e comunicações:** análise de procedimentos operacionais e responsabilidades, planejamento e aceitação do sistema (planejamento de capacidade, testes de aceitação), proteção contra vírus, cópias de segurança, trilhas de auditoria,

gerenciamento de redes de comunicação de dados, segurança e manuseio de mídias, troca de informações e softwares entre organizações;

- **Controle de acesso:** sincronização dos relógios do sistema, monitoração de uso e acesso aos sistemas (logs), controle de acesso de sistema operacional, gerenciamento de acessos de usuários, responsabilidade do usuário, computação móvel e comunicação remota;
- **Aquisição, desenvolvimento e manutenção de sistemas de informação:** segurança sobre desenvolvimento, aquisição e manutenção de sistemas computacionais;
- **Gestão de incidentes de segurança da informação:** notificação de eventos de segurança da informação, gerenciamento de incidentes, coleta de evidências;
- **Gestão da continuidade do negócio:** análise das estratégias para continuidade dos negócios;
- **Compliance:** conformidade de requisitos legais e auditoria.

Cada um destes macro-controles é subdividido em vários outros, totalizando 153 controles de segurança, que visam manter e gerir a segurança da informação na organização. Maiores detalhes sobre estes controles podem ser obtidos na própria NBR (GONÇALVES, 2004).

1.4.2 Segurança da Informação

Antes de definir o que é segurança da informação, é oportuno esclarecer o que vem a ser um ativo. A norma NBR ISO/IEC 17799 define que numa rede de computadores podem existir quatro tipos de ativos:

- **Ativos de informação:** base de dados e arquivos, documentação de sistema, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de contingência, procedimentos de recuperação, informações armazenadas;
- **Ativos de *software*:** aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

- **Ativos físicos:** equipamentos computacionais (processadores, monitores, *laptops*, *modems*), equipamentos de comunicação (roteadores, PABX, fax, secretárias eletrônicas), mídia magnética (fitas e discos), outros equipamentos técnicos (*no-break*, ar-condicionado), mobília e acomodações;
- **Serviços:** computação e serviços de comunicação, utilidades gerais como, por exemplo, aquecimento, iluminação, eletricidade, refrigeração.

Utilizando como universo os quatro tipos de ativos listados acima e para delimitar o escopo de entendimento neste capítulo, serão abordados os problemas de segurança relacionados com a informação.

A mesma norma define a informação como um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e, conseqüentemente, necessita ser adequadamente protegida. A segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos e maximizar o retorno dos investimentos (ROI) e as oportunidades de negócio.

A informação pode existir em muitas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou usando meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Uma segurança da informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de *software*. Estes controles precisam ser estabelecidos para garantir que os objetivos de segurança específicos da organização sejam atendidos.

A NBR é composta por 153 controles distintos e o processo de seleção dos controles a ser aplicado nem sempre é fácil de ser realizado. Para (GONÇALVES, 2004), “para facilitar o processo de seleção de controles podemos utilizar algumas ferramentas, como por exemplo: a Análise de Risco de um ambiente, a Legislação Vigente, os Objetivos e Necessidades da organização”.

Da mesma forma que no mundo real as empresas se preocupam em proteger seu patrimônio contra os mais variados riscos, no mundo virtual a preocupação é a mesma com relação à informação.

O principal risco que a informação está exposta são os diversos tipos de ataques que são executados contra ela.

1.5 METODOLOGIA

1.5.1 Autorização para pesquisar

Considerando que o desenvolvimento deste trabalho está baseado no Departamento de uma instituição pública de ensino superior, foi necessário obter uma autorização para a pesquisa. O documento expedido pelo SENAC – Florianópolis pode ser verificado no Anexo I.

1.5.2 Caracterização da Pesquisa

Para o desenvolvimento deste Plano Estratégico, se faz necessária a obtenção de dados seguros, o que exige a escolha de um método de pesquisa que proporcione indicadores confiáveis à resolução do problema proposto.

A pergunta que serviu como tema deste trabalho foi: “Quais são os dados mais valiosos que o EQA possui?”. Para respondê-la foi escolhido, como técnica de pesquisa, o estudo de caso qualitativo, o qual é indicado em investigações que buscam responder a este tipo de questão (YIN, 1994).

1.5.3 Técnica de Coleta de Dados

Dentre as técnicas de levantamento de dados descritas por (MARCONI, 2009), este trabalho utilizou três, que foram:

a) **Documentação indireta**: Nesta técnica de pesquisa documental, foram pesquisados documentos oficiais escritos, tais como:

- **Tabela de Temporalidade**: documento que classifica e determina o tempo de permanência de cada tipo de documento nos órgãos da UFSC (DMSG, 2009);
- **Sites oficiais da UFSC** (UFSC(a), 2009) **e do EQA** (EQA, 2009): contêm páginas com informações de todos os setores da Universidade, com documentações oficiais públicas;
- **Documentos internos**: foram examinados documentos pertinentes à Política de Segurança da Informação, tais como a Portaria 337/GR/2007 (Anexo II), que cria o Núcleo de Inovação Tecnológica (NIT) e os Termos de Confidencialidade, destinados aos mestrandos e doutorandos (Anexo III) e pesquisadores (Anexo IV) que utilizam laboratórios do EQA, cujas pesquisas exigem sigilo.
- **Legislação Federal**: foram examinados diversos documentos oficiais, aplicáveis aos órgãos federais, tais como Leis, Decretos e Portarias, que regulam as boas práticas relativas à segurança da informação;
- **Fluxograma da informação**: análise do fluxograma da informação, com ênfase na área de pesquisa.

b) **Documentação direta:** Nesta técnica de pesquisa documental foram levantados dados, através da pesquisa de campo, no próprio local onde os fenômenos ocorrem (MARCONI, 2009, p.188), tais como:
   - **Parque tecnológico:** levantamento e análise dos dados do parque tecnológico;
   - **Registro fotográfico:** fotos da estrutura física da rede do EQA, produzidas durante a vistoria do local.

c) **Observação direta intensiva:** Nesta técnica optou-se pela entrevista despadronizada ou não-estruturada (MARCONI, 2009, p.199). A seleção do entrevistado foi baseada no método não probabilístico com amostragem intencional, uma vez que “a generalização, no sentido estatístico, não é o objetivo da pesquisa qualitativa” (MERRIAM, 1998, p.61). Além disso, alguns critérios foram estabelecidos para a escolha do entrevistado: deveria ter, no mínimo, dez anos de experiência na área de informática e, no mínimo, cinco anos no ambiente da UFSC, não

importando o fato de ser homem ou mulher (MORAES, 2000). Os entrevistados foram:

- Gerente do EQA;
- Coordenador de pesquisa do EQA;
- Coordenador do curso de pós-graduação do EQA;
- Supervisor de NDA;
- Coordenador do NPD.

Apesar dos prós e contras desta técnica, obtiveram-se as seguintes vantagens, limitações e superações:

- **Vantagens:**
  - Maior flexibilidade: O entrevistador pode repetir e/ou esclarecer as perguntas, e até mesmo formulá-las de maneira diferente. Isto facilitou o entendimento para ambos e, como resultado, obteve-se um melhor entendimento das medidas de segurança existentes no Departamento;
  - Oportunidade para obtenção de dados que não se encontram em fontes documentais e relevantes para o plano estratégico;
  - Possibilidade de obter informações mais precisas e que puderam ser comprovadas no desenvolvimento do plano estratégico.
- **Limitações:**
  - A retenção de alguns dados importantes foi inevitável, pois, por se tratar de um trabalho acadêmico, não poderiam ser revelados, para garantir a segurança da rede e da instituição;
  - Apesar da boa disposição dos entrevistados em fornecer o máximo de informações, a entrevista não pode se estender por um período muito longo, o que impediu que alguns temas fossem abordados com a devida profundidade, mas sem prejuízo à pesquisa.
- **Limites superados:**
  - Os entrevistados não foram influenciados (de forma consciente ou inconsciente) pelo entrevistador, principalmente por se tratar

de profissionais com larga experiência e vivência na área de informática e por conhecer profundamente o assunto abordado;
- Os entrevistados demonstraram boa disposição em fornecer as informações necessárias à pesquisa.

1.5.4 Forma de Análise dos Dados

Conforme sugerido por Merriam (1998), a análise dos dados foi iniciada enquanto se fazia a coleta dos mesmos, através de anotações em um diário de campo das observações e reflexões sobre o que estava se passando.

A categorização dos dados foi realizada baseada na *Grounded Theory*, de Glaser & Straus (1967), que ressalta duas estratégias importantes.

A primeira é o método constante de comparação, na qual o pesquisador simultaneamente codifica e analisa os dados coletados para criar conceitos. Através de constantes comparações de incidentes específicos nos dados, o pesquisador refina estes conceitos, identifica as propriedades, explora a relação entre os dados e as integra em uma teoria coerente.

A segunda é o método da amostragem teórica, na qual o pesquisador seleciona novos casos de estudo com o potencial dos mesmos em ajudar a expandir ou refinar os conceitos e teorias já criados previamente.

A *Grounded Theory* permite captar a essência do fenômeno, dando sentido aos dados coletados através do “agrupamento de conceitos que parecem pertencer ao mesmo fenômeno” (STRAUSS e CORBIN, 1990, p.65). Isso exige a comparação constante dos dados, um movimento de “ir e vir entre pedaços concretos de dados e conceitos abstratos, entre o raciocínio indutivo e dedutivo, entre a descrição e a interpretação” (MERRIAM, 1998).

A validade dos dados, ou seja, o quanto as descobertas são coerentes com a realidade, foi assegurada através da ratificação dos dados levantados pelos entrevistados. Contudo, apesar do rigor metodológico, adverte-se que esse método não exclui a possibilidade de vieses na interpretação dos dados (MERRIAM, 1998).

1.6 OBJETIVO DO ESTUDO

1.6.1 Apresentação da Empresa

O Departamento de Engenharia Química e Engenharia de Alimentos faz parte do centro tecnológico da Universidade Federal de Santa Catarina UFSC.

O curso de Engenharia Química da Universidade Federal de Santa Catarina foi criado em 13 de outubro de 1978, pela Portaria 428/GR/78, tendo obtido seu reconhecimento em 11 de janeiro de 1985, conforme Portaria 006/MEC/85.

O objetivo geral do Curso de Engenharia Química da UFSC é formar profissionais, engenheiros químicos, capazes de desempenhar eficientemente suas tarefas, atendendo às exigências atuais do mercado de trabalho. Mais especificamente, o Curso de Engenharia Química pretende preparar profissionais para atuarem em vários setores industriais da área química, podendo atuar como Engenheiros de Projetos, Engenheiros de Processo e de Produção, trabalhando no desenvolvimento e aprimoramento de novos processos, bem como na pesquisa de novos produtos.

O Departamento de Engenharia Química e Engenharia de Alimentos é o principal responsável pela parte profissionalizante do curso. Estão lotados neste departamento 29 professores de dedicação exclusiva, dos quais 3 são mestres, e todos os demais doutores. O EQA conta temporariamente com 2 professores substitutos, sendo um doutor e o outro doutorando, e com mais um professor pesquisador.

O Departamento de Engenharia Química e Engenharia de Alimentos da UFSC também atua no Programa de Pós-Graduação em Engenharia Química, que surgiu em 1993, como uma conseqüência natural da qualificação do seu corpo docente, aliada à estruturação física de suas dependências. O programa oferece curso de Mestrado e Doutorado em Engenharia Química e tem uma interação bastante grande com o curso de graduação.

O curso de graduação em Engenharia de Alimentos da Universidade Federal de Santa Catarina foi criado em agosto de 1979, tendo obtido seu reconhecimento em 14 de março de 1985.

A logomarca do EQA, que por muitos anos foi vinculada ao curso, foi criada

em 1989, numa busca bem humorada de representar a complexidade e diversidade do Engenheiro de Alimentos.

O objetivo geral do curso é formar profissionais capacitados para atuar em processos de transformação industrial de alimentos, desde a seleção da matéria-prima adequada à industrialização, passando por todas as etapas do processo e pela definição das melhores condições de distribuição e de armazenamento do produto acabado. Mais especificamente, o Curso de Engenharia de Alimentos da UFSC procura formar engenheiros capazes de contribuir para a melhoria e o desenvolvimento de novos processos de transformação de alimentos nos diferentes ramos da indústria de alimentos.

> Missão: Promover o desenvolvimento científico e tecnológico da Engenharia Química e Engenharia de Alimentos e a função social do engenheiro, através do ensino, pesquisa e extensão, buscando suprir as demandas da sociedade e a melhoria da qualidade de vida (EQA, 2009).

2 DIAGNÓSTICO

O Departamento apresenta algumas iniciativas pontuais de segurança da informação sem ter uma correlação sistêmica.

Após um levantamento da atual situação do Departamento podemos citar algumas iniciativas de segurança, tais como:

- Uma política de uso aceitável (AUP) destinada aos usuários do Departamento;
- Uma rotina de backup dos computadores da área administrativa;
- Um sistema de vigilância por imagens das áreas externas (Figura 2-1) do Departamento e interna do bloco E;

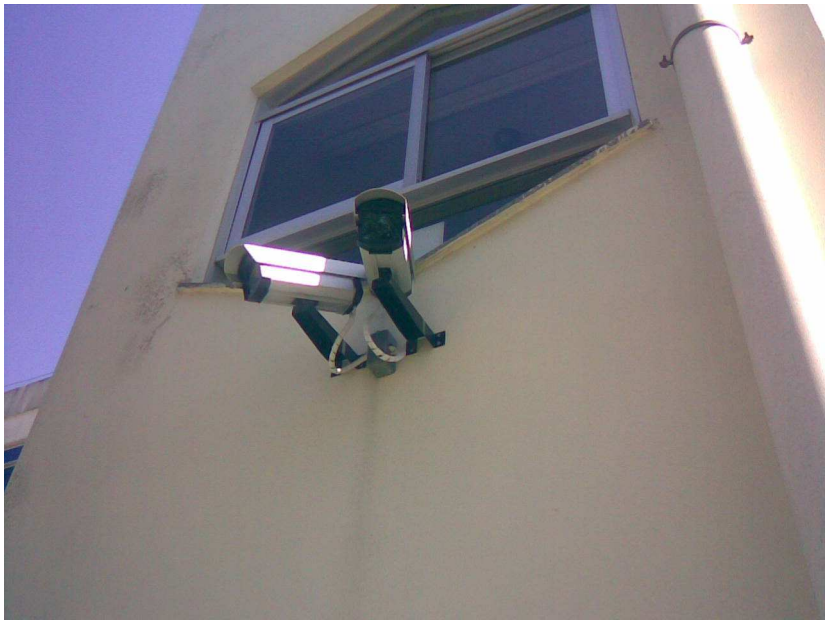


Figura 2-1: Sistema de monitoramento por imagens das áreas externas

- Restrição à circulação de pessoas não autorizadas em algumas áreas críticas (Figura 2-2), tais como a sala de meios (bloco E) e a sala de redes;

Figura 2-2: Restrição de acesso no bloco E

- Controle de acesso após expediente no bloco E.

Entretanto, estas abordagens pontuais não são suficientes para caracterizar uma política de segurança da informação no Departamento.

2.1 CARACTERIZAÇÃO DO AMBIENTE EXTERNO

Campus da Universidade, comunidade universitária e comunidade local (cidades sede do campus). O mapa da UFSC está representado na Figura 2-3.

Figura 2-3: Mapa da UFSC

2.1.1 Macro Ambiente

- O Estado de Santa Catarina;
- O Município de Florianópolis
- Campus da Universidade Federal do Estado de Santa Catarina (UFSC);
- Centro Tecnológico (CTC);
- Departamento de Engenharia Química e Engenharia de Alimentos (EQA).

2.1.1.1 Forças Legais

- Constituição da República Federativa do Brasil 1988;
- Lei 8.112, de 11 de dezembro de 1990, dispõe sobre o regimento jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;
- Estatuto da ética dos servidores da UFSC;
- Portarias (legislação) expedidas por:
    - Ministro da Educação;
    - Secretário da Educação;
    - Reitor;
    - Vice Reitor;
    - Pró Reitores;
    - Diretor do CTC;
    - Chefe do EQA.
- Portarias decorrentes de setores administrativos como:
    - Divisão de Segurança e Saúde do Trabalhador (DSST);
    - Departamento de Recursos Humanos (DRH).
- Lei 9.983, de 14 de julho de 2000, que altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal e dá outras providência;
- Dispositivos legais de caráter Federal (Anexo V);
- Legislação específica de caráter:
    - Federal (Anexo VI);
    - Estadual / Distrital (Anexo VII);

- Municipal (Anexo VIII).
- Normas técnicas (Anexo IX).

2.1.1.2 Forças Políticas

A cada quatro anos há troca dos dirigentes e, conseqüentemente, mudança do quadro administrativo (direção, cargos comissionados, chefia).

Organizações sindicais (em ordem alfabética):

- ANDES;
- APUFSC;
- CONLUTAS;
- CUT;
- FASUBRA;
- SINTUFSC.

Determinações e políticas advindas do alto escalão da administração pública (presidência da república, ministros, diretores e secretariados).

2.1.1.3 Forças Econômicas

Orçamento da União para a Educação, incentivo das Empresas privadas às pesquisas e agentes financiadores de fomentação a pesquisa (CAPES, FINEP, CNPq).

Outros fatores são a conjuntura econômica mundial e nacional que têm influenciado na qualidade e quantidade dos projetos de pesquisa e nos aportes financeiros no desenvolvimento destas pesquisas no EQA.

2.1.1.4 Forças Tecnológicas

Políticas definidas pelo Ministério da Educação, políticas técnico-administrativas do NPD e NDA da UFSC.

Outro fator também importante é a influência mundial no desenvolvimento de tecnologias aos meios acadêmicos, no que tange a disponibilidades e a velocidade do surgimento de novas tecnologias.

2.1.1.5 Forças Ecológicas

Políticas governamentais definidas pelos órgãos competentes (IBAMA, FATMA e plano diretor municipal).

Esta é uma força bem atuante nos dias atuais, demonstrando a preocupação da comunidade com a preservação do meio ambiente e o desenvolvimento sustentável.

2.1.1.6 Forças Culturais

Referências culturais provenientes de povos vindos da Europa, africanos e povos indígenas.

2.1.1.7 Forças Sociais

O ambiente de trabalho, por ser regido pelo Regime Jurídico Único (RJU), identifica certa ingerência no comportamento dos funcionários na óptica da obediência das normas, portarias e legislação que regem o ambiente organizacional do Departamento.

Uma Universidade sugere a sensação de liberdade, sem restrições, o que dificulta a implantação de qualquer norma ou política restritiva.

Com relação à segurança da informação, por ser um ambiente acadêmico (universitário) a organização não possui uma grande preocupação ou cuidado com a segurança de suas informações. Isto pode ser comprovado com os índices baixos de patentes realizados no Brasil em relação a outros países.

2.1.1.8 Forças Demográficas

Demografia (Demo = povo, Grafia = estudo), segundo (WIKIPEDIA(a), 2009), “é o estudo do povo/população. A demografia é um estudo que engloba desde estudos individuais e dependentes até projetos do governo em relação à população, como o IDH”.

Apesar de existirem 10 instituições de ensino superior públicas em Santa Catarina (WIKIPEDIA(b), 2009) é grande a procura da comunidade às vagas oferecidas pela UFSC. Os dados estão no relatório emitido pela COPERVE (COPERVE, 2009) referente aos últimos 10 anos. A Figura 2-4 apresenta a página 18 deste relatório e na Figura 2-5 é possível verificar a evolução da relação candidato/vaga para os cursos do EQA.

UNIVERSIDADE FEDERAL DE SANTA CATARINA
COMISSÃO PERMANENTE DO VESTIBULAR
Vestibular 2009

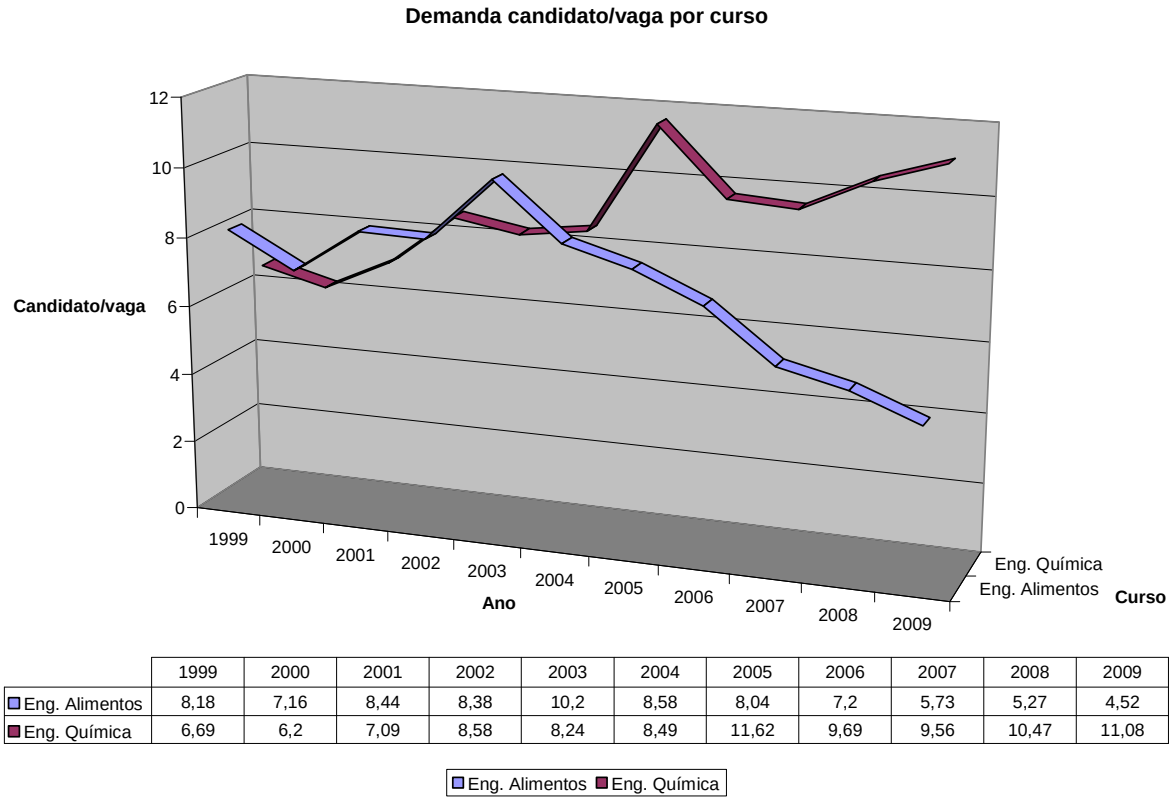
Demanda candidatos/vaga por curso no período de 1999 a 2009

Curso	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
ENGENHARIA CIVIL	6.88	5.08	5.84	7.38	6.86	7.12	7.42	5.68	6.71	6.84	10.56
ENGENHARIA DE ALIMENTOS	8.18	7.16	8.44	8.38	10.20	8.58	8.04	7.20	5.78	5.27	4.52
ENGENHARIA DE AQÜICULTURA	4.85	6.13	7.10	6.57	7.33	7.67	7.90	4.93	4.38	2.67	3.04
ENGENHARIA DE MATERIAIS	3.22	4.55	4.73	4.63	3.40	4.45	5.02	4.38	4.13	3.17	3.78
ENGENHARIA DE PRODUÇÃO CIVIL	3.37	6.57	2.94	9.37	3.51	5.14	5.03	4.69	4.20	4.48	6.13
ENGENHARIA DE PRODUÇÃO ELÉTRICA	3.71	7.66	4.37	7.09	4.43	4.60	5.54	4.43	3.37	4.18	3.40
ENGENHARIA DE PRODUÇÃO MECÂNICA	5.54	7.23	6.17	7.20	6.89	7.23	9.00	9.63	8.49	7.38	8.45
ENGENHARIA ELÉTRICA	8.04	6.75	8.53	11.72	9.33	7.62	7.47	5.58	5.52	5.00	5.32
ENGENHARIA MECÂNICA	7.49	6.62	8.98	9.56	10.46	10.28	12.28	11.60	11.02	11.17	10.72
ENGENHARIA QUÍMICA	6.69	6.20	7.09	8.58	8.24	8.49	11.62	9.69	9.56	10.47	11.08
ENGENHARIA SANITARIA E AMBIENTAL	3.59	5.83	6.09	6.43	11.74	8.40	8.26	7.41	6.93	8.48	7.16

Obs.: Os candidatos inscritos por experiência não fazem parte desta estatística.

Figura 2-4: Relatório da COPERVE

No gráfico da Figura 2-5 observa-se que o curso de Engenharia de Alimentos teve um aumento de procura entre 1999 e 2003, mas vem perdendo candidatos de 2004 até 2009. A Engenharia Química teve um aumento gradativo de candidatos entre 1999 e 2005, e esta relação tem se mantido estável até 2009.



	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009
Eng. Alimentos	8,18	7,16	8,44	8,38	10,2	8,58	8,04	7,2	5,73	5,27	4,52
Eng. Química	6,69	6,2	7,09	8,58	8,24	8,49	11,62	9,69	9,56	10,47	11,08

Figura 2-5: Gráfico da demanda candidato/vaga do EQA

Florianópolis está se caracterizando por um centro de excelência na área de educação, ocorrendo uma grande concentração de acadêmicos, professores, pesquisadores e cientistas.

> O aglomerado urbano de Florianópolis (Florianópolis, Biguaçu, Palhoça e São José) totaliza uma população estimada para 2002 de 702.988 habitantes, segundo o IBGE. Florianópolis, apesar de ser a capital do Estado, não é a sua maior cidade, tendo uma população inferior a de Joinville, que tem uma estimativa para 2002 de 453.766 habitantes segundo IBGE.
> Florianópolis, cidade pólo do aglomerado urbano, tem uma população estimada de 360.601 habitantes em 2002/IBGE. A população total do aglomerado representa 94,10% da população total do Núcleo da Região Metropolitana (747.021 habitantes), esta por sua vez representa 13,51% da população de Santa Catarina. Em janeiro de 1998, a Lei Complementar nº 162 instituiu a Região Metropolitana de Florianópolis, a primeira a ser criada no Estado com objetivo principal de dinamizar as soluções dos problemas urbanos comuns.
> O Município de Florianópolis é composto por 12 distritos que se concentram na Ilha. Segundo dados do IBGE de 2000, destaca-se o distrito sede com maior população (213.574 habitantes). Em média, cada distrito possui 9.127 habitantes. A Ilha possui 85 comunidades, sendo a comunidade do Centro a com o maior número de habitantes

(41.827). No Continente, que possui 9 comunidades, Capoeiras é o mais populoso, com 17.905 habitantes, enquanto que a comunidade de Bom Abrigo perfaz 1.196 habitantes.
A densidade demográfica de Florianópolis em 2000 corresponde a 760,10 hab/km2 (PMF, 2009).

2.1.2 Ambiente Específico

A caracterização do ambiente específico corresponde à seguinte estrutura:

- República Federativa do Brasil;
- Ministério da Educação (MEC);
- Universidade Federal de Santa Catarina (UFSC);
- Centro Tecnológico (CTC);
- Departamento de Engenharia Química e Engenharia de Alimentos (EQA);
- Unidade administrativa de laboratório.

2.1.2.1 Principais Fornecedores e Insumos

Os principais fornecedores são os patrocinadores, empresas ou entidades que desejam patrocinar as pesquisas e projetos e o Governo do Estado de Santa Catarina (através da FAPESC);

Os insumos são os temas e idéias transformadas em artigos, registro de patentes, relatórios técnicos, publicações acadêmicas (monografias, dissertações e teses) ou outras formas de publicações.

No fluxograma do processo de pesquisa (Figura 2-6) é possível verificar o processo de transformação destes insumos.

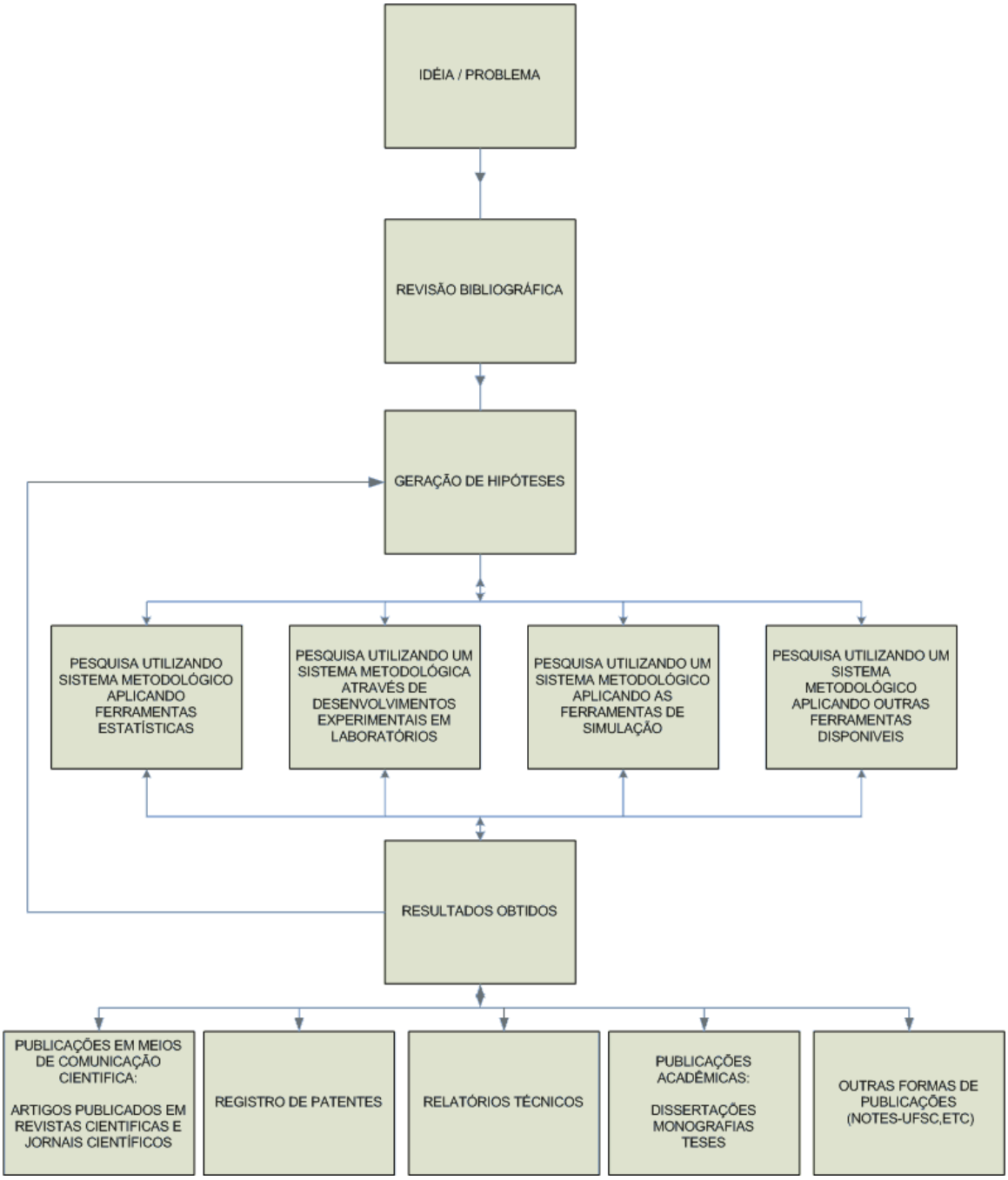


Figura 2-6: Fluxograma da pesquisa

2.1.2.2 Principais Empresas Concorrentes

As principais concorrentes do EQA são as instituições de ensino de nível superior nacional, tais como (em ordem alfabética):

- CESUSC;
- COPPE;

- IF-SC;
- SENAI;
- UDESC;
- UNISUL;
- UNIVALI;
- e outras.

Além destas, também entram na lista:

- Instituições de Educação de nível superior internacionais;
- Centros de pesquisas nacionais;
- Centro de pesquisas internacionais;
- Nações com grande interesse na obtenção de patentes com o objetivo de criar uma reserva de mercado para futuras explorações. Alguns exemplos seriam: Estados Unidos da América, Japão, Alemanha, entre outras.

2.1.2.3 Órgãos Reguladores e Fiscalizadores do Segmento

Os principais órgãos reguladores são:

- Ministério da Educação;
- Financiadora de Estudos e Projetos (FINEP);
- Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES);
- Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq);
- Empresas parceiras.

2.1.2.4 Principais Organizações que Atuam Como Parceiras

Fundações:

- Fundação de Estudos e Pesquisas Sócio-Econômicos (FEPESE);
- Fundação de Ensino e Engenharia de Santa Catarina (FEESC);
- Fundação Centros de Referência em Tecnologia Inovadora (CERTI);
- Fundação José Arthur Boiteaux (FUNJAB).

Empresas:

- Petrobras;
- Embraco;
- Sadia;
- CNPq;
- FINEP;
- CAPES.

2.1.2.5 Mercado Tecnológico

Possui soluções engessadas e com alto valor comercial, inviável para o “caso”.

Numa instituição pública as aquisições de tecnologia e equipamentos são realizadas via pregões e licitações, obedecendo, portanto, à lei do menor preço, conseqüentemente não segue um padrão pré-definido.

Qualquer empresa pode ser fornecedora desde que preencha os requisitos obrigatórios no registro de cadastro (SICAF).

A Lei 8.666, de 21 de junho de 1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.

2.1.2.6 Mercado de Informação

As informações são coletadas pelos pesquisadores da seguinte forma:

- Consulta aos professores titulares dos temas desenvolvidos;
- Levantamento bibliográfico a livros da área;
- Consulta a teses e dissertações que desenvolveram o tema da pesquisa;
- Pesquisa a artigos de periódicos e revistas;
- Participações em congressos da área para verificar que caminho os colegas da área estão tomando (benchmarking);
- Consulta a outros centros de pesquisa nacionais e internacionais;
- Cursos e treinamentos técnicos.

Os resultados finais das pesquisas são:

- Monografias, teses, dissertações;
- Relatórios de consultoria;
- Artigos públicos em veículos próprios;
- Patentes.

A administração da UFSC disponibiliza estas informações através da Biblioteca Central, através de vários convênios, tais como assinatura de revistas, periódicos e outros, além de possuir um vasto acervo bibliográfico incluindo monografias, teses e dissertações, disponíveis para os pesquisadores.

A administração presta auxílio através do fornecimento de passagens e pagamento de diárias, para os pesquisadores participarem de congressos nacionais e internacionais.

2.1.3 Principais Tendências Culturais e Tecnológicas em Relação à Segurança da Informação

Gabinete de Segurança Institucional (GS)I: Gabinete vinculado à Presidência da República, tem como função definir as políticas de segurança da informação na administração pública. Pela Medida Provisória (MP) 1.911-10, de 24 de setembro de 1999, que altera dispositivos da Lei 9.649, de 27 de maio de 1998, passou à Casa Militar a chamar-se Gabinete de Segurança Institucional. No art. 24-A, criou-se o cargo de Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República.

INSTRUÇÃO NORMATIVA GSI Nº1, de 13 de junho de 2008: Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

Comitê Gestor da Segurança da Informação: Criado pelo Decreto 3.505 de 13 de junho de 2000, o Comitê Gestor da Segurança da Informação assessora a Secretaria Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto.

Decreto 3.505, de 13 de junho de 2000: Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

Lei 9.610, de 19 de fevereiro de 1998: Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências.

2.2 CARACTERIZAÇÃO DO AMBIENTE INTERNO

O ambiente interno caracteriza-se por um nível baixo de controle de segurança da informação, sendo que as ações são pontuais, não apresentando conexão (sistêmico).

O Orçamento é insuficiente para atender todas as demandas referentes à Tecnologia da Informação.

2.2.1 Ambiente Organizacional

O ambiente organizacional corresponde a um modelo clássico de administração. O organograma é hierárquico e departamentalizado.

Organizado através de normativa, criada internamente e imposta pelo Ministério da Educação.

2.2.1.1 Situação nos Negócios

Conforme pode ser verificado na Tabela 2-1, a UFSC está entre as 15 melhores Universidades do Brasil.

O programa de pós-graduação em engenharia química e engenharia de alimentos tem conceito 5 na CAPES.

Tabela 2-1: Grande Área da Engenharia Química

PROGRAMA	IES	UF	CONCEITO			Ranking
			M	D	F	
Des. de Processos Ambientais	UNICAP	PE	3	-	-	1º
Engenharia de Processos	UFCG	PB	-	3	-	2º
Engenharia de Processos	UFSM	RS	3	-	-	3º
Engenharia de Processos	UNIVILLE	SC	3	-	-	4º
Engenharia de Processos	UNIT-SE	SE	3	-	-	5º
Engenharia de Processos Químicos e Bioquímicos	CEUN-IMT	SP	3	-	-	6º
Engenharia de Processos	UFAL	AL	3	-	-	7º
Engenharia Química	UFBA	BA	3	-	-	8º
Engenharia Química	UFBA	BA	-	4	-	9º
Engenharia Química	UFC	CE	4	4	-	10º
Engenharia Química	UFSC	SC	5	5		25º
Engenharia Química	FURB	SC	3	-	-	26

Fonte: CAPES (CAPES, 2009).

2.2.1.2 Investimentos em Tecnologia

Da mesma forma que todas as instituições públicas, a UFSC têm seus gastos previstos em orçamentos anuais.

O orçamento é elaborado pela Administração Central, através da Secretaria de Planejamento e Finanças, e encaminhado ao Conselho Universitário para aprovação.

Conforme publicado em (UFSC(b), 2009) e disponível na Figura 2-7, é possível verificar o orçamento previsto para o item “Ações de Informática”, na linha referente à coluna PTRES 024764. O valor total estimado para 2009 é de R$ 730.000,00 (setecentos e trinta mil reais).

UNIVERSIDADE FEDERAL DE SANTA CATARINA
SECRETARIA DE PLANEJAMENTO E FINANÇAS
DEPARTAMENTO DE GESTÃO ORÇAMENTÁRIA
PROPOSTA ORÇAMENTÁRIA 2009
LEI Nº 11.897 de 30/12/2008

					LIMITE	TOTAL
			TRANSPORTE		558.367.993,00	558.367.993,00
PTRES	PROG.DE TRABALHO	ESPECIFICAÇÃO	NATUREZA	FTE	LIMITE	TOTAL
002410	12.364.1073.4009.0042	FUNCIONAMENTO DE CURSOS DE GRADUAÇÃO	3390.14	112	605.000,00	
		- MANUTEÇÃO DO ENSINO	3390.14	250	160.000,00	
			3390.39	112	4.038.372,00	6.847.965,00
024765	12.364.1073.11JK.0042	Reestruturação e Expansão das Universidades Federais - REUNI	4490.51	112	12.641.632,00	
			4490.52	112	3.000.000,00	15.641.632,00
025924	12.364.1073.11JK.0042	Reestruturação e Expansão das Universidades Federais - REUNI	4490.51	312	2.310.701,00	
				0		2.310.701,00
024764	12.126.075.2003.0001	ACOES DE INFORMATICA	3390.39	112	130.000,00	
			4490.52	112	600.000,00	730.000,00
026598	12.391.0167.4013.056	PRESERVACAO DE ACERVOS HISTORICOS, AD-MUSEU UNIVERSITÁRIO	4490.00	100	400.000,00	400.000,00
026597	12.364.1073.2E14.0248	REFORMA E MODERNIZACAO DE INFRA-ESTRU - NO ESTADO SC	4490.00	100	300.000,00	300.000,00
			TOTAIS		661.863.953,00	661.863.953,00

Figura 2-7: Orçamento 2009 - UFSC

No EQA existe um planejamento de reestruturação física da rede (switch, servidores, impressoras de rede, etc.) vigente para o período de 2008 a 2011 que corresponde ao planejamento estratégico do Departamento.

2.2.1.3 Disposição do Espaço Físico

O Departamento é constituído de oito blocos (blocos A, B, C, D, E, de sala de aula, e os novos I e II). As funcionalidades de cada bloco são as seguintes:

- Administrativo: Bloco E.

Neste bloco estão as coordenadorias dos cursos de graduação e pós-graduação onde são processados os documentos dos acadêmicos (conceito, histórico, programa, atestado de freqüência, memorandos, portarias, etc.).

- Laboratórios: Blocos A, B, C, D e os novos I e II.
  Em cada um destes blocos estão localizados os laboratórios vinculados aos programas de pós-graduação do EQA, que são:
  a) Curso de Pós-Graduação em Engenharia Química (CPGENQ);
  b) Curso de Pós-Graduação em Engenharia de Alimentos (CPGEA).
- Salas de aula: Blocos E e de salas de aula.
  As salas de aula são destinadas aos acadêmicos dos cursos de graduação e pós-graduação, dos cursos de engenharia química e engenharia de alimentos, e eventualmente atende outros cursos da UFSC.

2.2.2 Ambiente Informacional

O EQA tem como missão Promover o desenvolvimento científico e tecnológico da Engenharia Química e Engenharia de Alimentos e a função social do engenheiro, através do ensino, pesquisa e extensão, buscando suprir as demandas da sociedade e a melhoria da qualidade de vida.

2.2.2.1 Estratégia Informacional

O EQA possui programas de pós-graduação (mestrado e doutorado) em Engenharia Química (CPGENQ, 2009) e Engenharia de Alimentos (CPGEA, 2009), cujas estratégias informacionais estão listadas a seguir:

- **Estratégia informacional do Curso de Pós-Graduação em Engenharia Química (CPGENQ):**
  - Linhas de pesquisa do CPGENQ:
    - Engenharia de Reações Químicas e Desenvolvimento de Materiais:

- Pirólise e gaseificação de carvão mineral;
- Catálise ambiental;
- Desativação e regeneração de catalisadores;
- Reatores heterogêneos;
- Processos sol-gel;
- Materiais cerâmicos;
- Desenvolvimento de materiais bactericidas;
- Otimização energética e controle de emissões em queimadores de fonte fixa;
- Processos avançados de oxidação;
    - Laboratórios e Grupos:
        - Laboratório de Energia e Meio Ambiente – LEMA;
        - Laboratório de Materiais e Corrosão – LABMAC.

- Engenharia Genômica e Engenharia Biomédica:
    - Bioinformática;
    - Engenharia metabólica;
    - Genômica funcional e estrutural;
    - Engenharia de tecidos;
    - Neuroengenharia;
    - Modelagem matemática de processos neurobiológicos;
    - Fluxo sanguíneo cerebral e metabolismo;
    - Arquitetura de redes de neurônios;
        - Laboratórios e Grupos:
            - Laboratório de Neuroengenharia Computacional – NEUROLAB;
            - Laboratório de Tecnologias Integradas – INTELAB.
- Fenômenos de Transporte e Meios Porosos:
    - Desenvolvimento de métodos numéricos;
    - Experimentação, modelagem e simulação de problemas de transferência de calor, massa e quantidade de movimento em meios porosos, reatores químicos e biorreatores;

- Processos da indústria têxtil;
- Processos da indústria petroquímica, petróleo e gás;
- Processos da indústria de papel e celulose;
- Produtos naturais;
- Processos de alimentos;
- Racionalização e reuso de águas;
- Problemas ambientais;
    - Laboratórios:
        - Laboratório de Simulação Numérica de Sistemas Químicos – LABSIN;
        - Laboratório de Sistemas Porosos – LASIPO;
        - Laboratório de Transferência de Massa – LABMASSA.

- Modelagem, Otimização e Controle de Processos:
    - Otimização de produção em plantas de multipropósito;
    - Otimização e controle de processos fermentativos;
    - Otimização e controle de plantas de extração supercrítica;
    - Modelagem estatística em substratos fractais;
    - Desenvolvimento de estratégias de controle de processos;
    - Inteligência artificial aplicada;
    - Dinâmica e controle de reatores de polimerização;
    - Controle de processos aplicado à indústria de petróleo e gás natural;
    - Modelagem e identificação de processos;
        - Laboratórios:
            - Laboratório de Controle de Processos – LCP;
            - Processos Biotecnológicos;
            - Termodinâmica e Processos de Separação.
- Processos Biotecnológicos:
    - Cultivo de células em biorreatores não-convencionais;
    - Produção de aromas e pigmentos via processos biotecnológicos;
    - Produção de biopolímeros;

- Valorização biotecnológica de resíduos agroindustriais;
- Catálise enzimática;
- Tratamento biológico de resíduos;
- Remoção biológica de nutrientes;
- Recuperação avançada de petróleo por processos biológicos.
    - Laboratórios:
        - Laboratório de Engenharia Bioquímica – ENGEBIO;
        - Laboratório de Tratamento Biológico de Resíduos - LTBR

- Termodinâmica e Processos de Separação:
    - Determinação experimental de dados de equilíbrio de fases;
    - Predição de propriedades termodinâmicas e de transporte;
    - Extração supercrítica de aromas e essências;
    - Síntese de sistemas de separação;
    - Processos de separação por membranas, adsorção, destilação e extração;
    - Valorização de produtos derivados de celulose e papel;
    - Separação de terpenos e terpenóides.
        - Laboratórios e Grupos:
            - Laboratório de Transferência de Massa – LABMASSA;
            - Laboratório de Controle de Processos – LCP.

- **Estratégia informacional do Curso de Pós-Graduação em Engenharia Química (CPGEA):**
    - Linhas de Pesquisa CPGEA:
        - Transferência de Calor e Massa no Processamento de Alimentos;
        - Processos de Separação: Extração Supercrítica e Separação com Membranas;
        - Processos Biotecnológicos e Cinética Microbiana Aplicada;

- Desenvolvimento de Processos e Produtos.

o Projetos de Pesquisa:

- Desenvolvimento, otimização e controle de processos;
- Produção de Aromas e Polímeros por Via Biotecnológica;
- Desenvolvimento de Tecnologias Limpas;
- Transferência de Calor e Massa Aplicada;
- Reologia e Propriedades Físicas de Alimentos;
- Secagem e Desidratação de Alimentos;
- Resfriamento e Congelamento de Alimentos;
- Processos de Separação com Membranas;
- Extração Supercrítica de Produtos Naturais;
- Desenvolvimento de Biofilmes de Amido e Proteínas;
- Desenvolvimento de Novos Produtos.

2.2.2.2 Política da Informação

Crescendo e aumentando cada vez mais o consumo da tecnologia que controla, classifica e armazena a informação, entende-se ser importante a normatização do trato deste ativo com procedimentos de classificação com relação ao seu grau de criticidade, manipulação e backups.

A política da informação na administração pública federal é definida pelo Gabinete de Segurança Institucional da Presidência da República, por intermédio do Departamento de Segurança da Informação e Comunicações, órgão este vinculado direto à Presidência da República, onde é definida a legislação que trata sobre as políticas da informação junto às repartições públicas federais.

2.2.2.3 Cultura e Comportamento em Relação à Informação

Áreas de conhecimento e pesquisa são bem definidas havendo, em alguns momentos, conflitos quando ocorre invasão de área por outra equipe.

Conforme o tipo de projeto de pesquisa existe um tratamento com relação às informações pertinentes ao projeto.

Para alguns são definidas políticas referentes à disponibilização de informações e restrição de acesso, geralmente solicitadas pelos parceiros quando o projeto tem potencial para gerar uma patente.

No trato da informação, o Departamento de Inovação Tecnológica (DIT, 2009) orienta aos pesquisadores de como tratar a informação nos projetos de pesquisa.

2.2.2.4 A Equipe Especializada em Informação

O Núcleo de Processamento de Dados (NPD) e o Núcleo de Desenvolvimento e Assessoramento Técnico (NDA) respondem pela equipe especializada em informação no Departamento.

As informações geradas nas pesquisas são de responsabilidade do coordenador de projeto, em que o mesmo armazena estas informações no ambiente corporativo denominado **NOTES UFSC,** e o coordenador acessa este ambiente através de login/senha**.** O serviço deste ambiente é disponibilizado on-line através de um servidor que fica localizado no prédio do NPD, o qual é submetido a processos de redundância da informação.

2.2.2.5 Processos de Gerenciamento da Informação

Processo I (acadêmico):

- Desenvolvimento das pesquisa/trabalho;
- Elaboração das dissertação/monografias/relatórios;
- Armazenamento na secretaria do curso de pós-graduação (um exemplar em papel e outro em mídia CD/DVD);
- Armazenamento nas bibliotecas (um exemplar em papel e outro em mídia CD/DVD).

Processo II (administrativo):

- Desenvolvimento das rotinas administrativas;
- Trato da informação conforme a Tabela de Temporalidade (DMSG, 2009);
- Armazenamento na CPU e no sistema;

- Backup.

Processo III (pesquisas):

- Geração das informações (relatórios);
- Administração do coordenador de projeto;
- Armazenamento no sistema NOTES – UFSC;
- Backup do servidor NOTES – UFSC.

O gerenciamento das informações na UFSC é definido pela legislação a seguir:

- **Lei 8.159, de 08 de janeiro de 1991:** Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.
- **Decreto 4.073, de 03 de janeiro de 2002:** Regulamenta a Lei 8.159, de 08 de janeiro de 1991.
- **Decreto 2.134, de 24 de janeiro de 1997:** Regulamenta o art. 23 da Lei 8.159, de 08 de janeiro de 1991, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências.

Existe uma comissão permanente de avaliação de documentos com as seguintes atribuições:

- Revisão e adaptação da Tabela de Temporalidade da UFSC (DMSG, 2009);
- Orientar a sua aplicação, dirimindo possíveis dúvidas;
- Orientar o processo de seleção dos documentos;
- Proceder à revisão periódica dos documentos relativos às atividades meio.

Os Departamentos da UFSC utilizam como referência para o trato da informação, a Tabela de Temporalidade.

> Tabela de Temporalidade é o instrumento de destinação, aprovado por autoridade competente, que determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documentos. A Tabela

> de Temporalidade poderá ser apresentada de duas formas: Tabela de Temporalidade de Atividade Meio e Tabela de Temporalidade de Atividade Fim (DMSG, 2009).

2.2.2.6 Arquitetura da Informação

Através de um levantamento visual no Departamento no EQA, constataram-se deficiências de:

- Segurança patrimonial;
- Controle de acesso físico;
- Controle de acesso lógico;
- Controle de armazenamento;
- Instalação da rede física.

2.2.3 Relatório Técnico da Estrutura de Redes

2.2.3.1 Diagrama da Topologia de Rede

A rede lógica do EQA, representada através da Figura 2-8, supre a comunicação entre os ativos de rede dos cinco blocos do departamento e o NPD, utilizando-se do conjunto de protocolos TCP/IP.

O projeto utiliza uma estrutura hierárquica e tem seu ponto central no Bloco D. Observando o desenho é possível identificar as três camadas dessa hierarquia:

- Camada Core: Localizada no Bloco D;
- Camada de distribuição: Localizada nos Blocos B, D e E.
- Camada de acesso: Identificada nos demais switches espalhados nos Blocos B, C, D e E.

Apesar das camadas estarem nitidamente identificadas, existem mais de três níveis de cascateamento, o que pode causar atrasos e dependências. Os switches foram distribuídos desordenadamente para atenderem necessidades locais e imediatas, gerando uma estrutura com muitos saltos nos Blocos D e E. A topologia utilizada é do tipo Hub-and-Spoke.

Existem dispositivos conectados a mais de uma camada, o que pode causar problemas inesperados de roteamento.

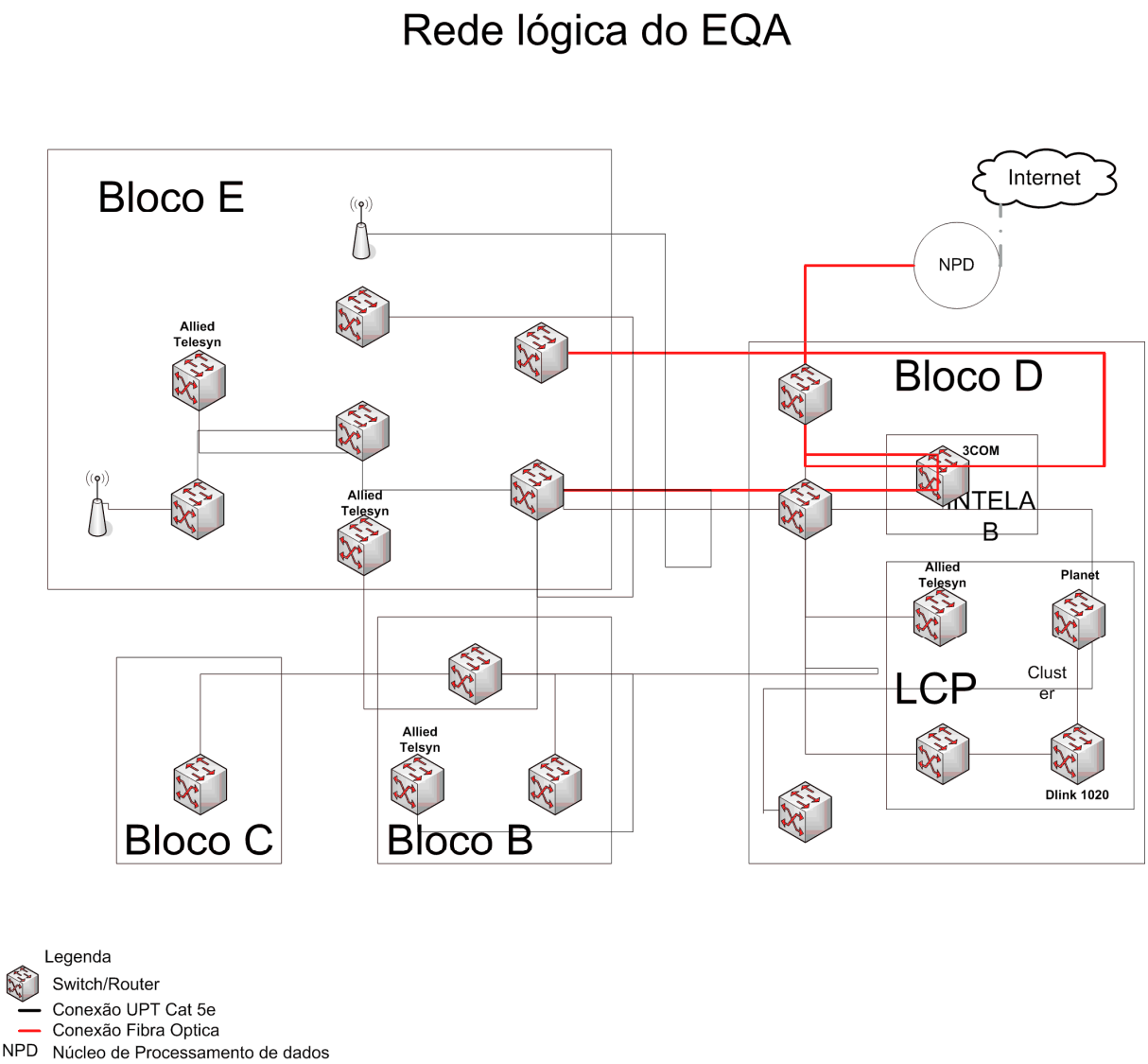


Figura 2-8: Rede lógica do EQA

2.2.3.2 Endereçamento de Rede

O EQA utiliza endereços IP públicos de classe B, com máscara de classe C (255.255.255.0).

As estações e servidores são endereçados de acordo com as VLANs definidas nesta rede. Existem cinco VLANs, identificadas no terceiro octeto, de acordo com a seguinte distribuição:

- **VLAN 70:** Denominada EQA, está localizada no Bloco E e atende à

administração do EQA e professores;

- **VLAN 71:** Denominada LCP, está localizada no Bloco D e atende ao laboratório dos professores Ricardo e Ariovaldo;
- **VLAN 72:** Denominada INTELAB, está localizada no Bloco D e atende ao laboratório dos professores Luismar e Leonel;
- **VLAN 73:** Denominada LABSIN, está localizada no Bloco E e atende aos professores;
- **VLAN 81:** Denominada ALUNOS, está localizada nos Blocos B e C e atende aos alunos e áreas comuns.

O serviço de resolução de nomes (DNS) é executado no NPD.

O esquema de roteamento não é complexo. Nos switches são utilizados protocolos Ethernet e Spanning Tree. Além destes, nos switches onde estão definidas as VLANs, é utilizado o protocolo Trunking.

Nos roteadores os protocolos são configurados, dependendo do tráfego:

- **Interno:** Para atender às necessidades de roteamento da rede do EQA são utilizados os protocolos RIP, IGRP e OSPF, dependendo da complexidade e quantidades de redes que serão roteadas;
- **Externo:** Os roteadores de borda utilizam protocolo BGP, por ser mais adequado à função que exerce.

2.2.3.3 Componentes de Rede

A rede é composta de ativos, como switches, roteadores e access points e passivos, tais como cabeamento, patch pannels, racks e nobreaks. Tais componentes são adquiridos através de licitação obedecendo a requisitos técnicos mínimos. Abaixo são apresentados os modelos dos principais componentes da rede:

- Switch E1 Matrix Gigabit 1G587-09;
- Switch 3COM 2016;
- Switch Allied Telesis AT-FS724L;
- Switch gerenciável Furukawa 5026;
- Switch gerenciável Planet FGSW-2620VM;
- Switch gerenciável Tiger SMC8024L2;

- Switch D-Link DES-1024D;
- Access Point wireless Linksys WRT54gs;
- Access Point wireless D-Link DWL-2100AP;
- Nobreak Power Sinus 3,2kVA.

2.2.3.4 Serviços de Rede Disponíveis

Os serviços de rede disponíveis estão distribuídos da seguinte forma:

- Bloco B - serviço FTP;
- Bloco D – serviço FTP e cluster;
- Bloco E – serviços FTP, HTTP e aplicativos;
- NPD – serviços FTP e correio eletrônico (IMAP, POP, SMTP);
- Demais Blocos – laboratórios;
- CIF´S;
- VPN.

2.2.4 Sistemas Operacionais e Aplicativos Utilizados

2.2.4.1 Sistemas Operacionais

O parque de máquinas do EQA é composto de estações de trabalho e servidores. A Tabela 2-2 apresenta os sistemas operacionais que estão instalados nestes equipamentos. Verifica-se que são utilizados sistemas operacionais livres e proprietários.

Tabela 2-2: Sistemas operacionais.

Sistema	Licenciamento	Aplicação
Microsoft Windows 2003 Server	Software proprietário	Servidores
Microsoft Windows XP	Software proprietário	Estações de trabalho
Open SUSE Linux	Software Livre	Servidores
Ubuntu	Software Livre	Estações de trabalho

2.2.4.2 Aplicativos

Para as atividades executadas no EQA são necessários diversos aplicativos para os mais variados objetivos. A lista destes softwares é apresentada na Tabela 2-3, onde pode ser verificada a presença de aplicativos livres e proprietários.

Tabela 2-3: Principais Aplicativos

Software	Licenciamento	Aplicação
Adobe Acrobat Reader	Software proprietário livre	Leitor de arquivos formato PDF
Adobe Acrobat Writer 5.0	Software proprietário	Gerador de arquivos formato PDF
Autocad	Software proprietário	Desenho técnico
Broffice.org	Software livre	Editoração de texto, planilha eletrônica, apresentação, etc.
CFX	Software proprietário	Simulador para área de engenharia
Estatística	Software proprietário	Auxiliar em métodos estatísticos
F-secure	Software proprietário	Antivírus
Matemática	Software proprietário	Auxiliar cálculos de engenharia
Matlab	Software proprietário	Voltado para cálculos numéricos e matrizes
Microsoft Office	Software proprietário	Editoração de texto, planilha eletrônica, apresentação, etc.
Pró-engineer	Software proprietário	Desenho técnico

2.2.5 Fatores Críticos de Sucesso em Relação à Segurança da Informação

> Os fatores críticos de sucesso, em inglês Critical Success Factor (CSF), 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 (WIKIPEDIA(c), 2009).

Os fatores críticos de sucesso para que este Plano Estratégico de Segurança da Informação seja bem sucedido, são:

- Comprometimento da Reitoria e da alta gerência;
- Política orçamentária da área;
- Patrocinadores;
- Comprometimento dos usuários do EQA;
- Disponibilidade de um profissional que dê continuidade ao plano de Segurança da Informação;
- Disponibilidade dos recursos tecnológicos;
- Planejamento estratégico eficiente.

3 ANÁLISE

3.1 ANÁLISE EXTERNA

3.1.1 Principais Oportunidades

A implantação de um plano de segurança da informação do Departamento EQA facilitará a associação com novos parceiros estratégicos que também se preocupam com o trato de suas informações num ambiente externo (principalmente espionagem de patentes).

Gerará também um maior crédito das ações do Departamento frente a Universidade.

3.1.2 Principais Ameaças

A principal ameaça corresponde à espionagem industrial e a incidentes que possam comprometer o desenvolvimento de patentes.

3.2 ANÁLISE INTERNA

3.2.1 Pontos Fortes

O Departamento já possui uma iniciativa no ambiente para proteção de suas informações, o que diminui bastante a rejeição à nova política que será proposta.

3.2.1.1 Aspectos Culturais / Comportamentais

O ambiente de uma universidade, em especial um laboratório, é constituído em sua maioria por profissionais com formação educacional, sendo na sua maioria composto por mestres e doutores, o que diminui bastante a rejeição cultural e comportamental para implantação de uma política de segurança.

3.2.1.2 Fontes de Poder e Política da Informação

- Agentes financiadores da pesquisa:
  - CAPES;
  - FINEP;
  - Empresas públicas;
  - Empresas privadas.
- Pró-reitoria de pós-graduação;
- Coordenadoria de pós-graduação;
- Coordenador do projeto de pesquisa.

3.2.1.3 Processos de Gerenciamento da Informação

Os processos estão definidos conforme:

- A Tabela de Temporalidade (DMSG, 2009);
- As leis:
  - **Lei 8.159,** de 08 de janeiro de 1991: Dispõe sobre a política nacional

de arquivos públicos e privados e dá outras providências;

- **Decreto 4.073**, de 03 de janeiro de 2002: Regulamenta a Lei 8.159, de 08 de janeiro de 1991;
- **Decreto 2.134**, de 24 de janeiro de 1997: Regulamenta o art. 23 da Lei 8.159, de 08 de janeiro de 1991, que dispõe sobre a categoria dos documentos públicos sigilosos e o acesso a eles, e dá outras providências.

- As determinações do Gabinete de Segurança Institucional da Presidência da República, por intermédio do Departamento de Segurança da Informação e Comunicações (DSIC, 2009);
- As determinações do Departamento de Inovação Tecnológicas (DIT, 2009) da UFSC.

3.2.1.4 Equipes de Profissionais

- Os profissionais do NPD/UFSC;
- A equipe do NDA/EQA/UFSC;
- Os profissionais do DIT/UFSC;
- Os bibliotecários e arquivistas do DMSG/UFSC.

3.2.1.5 Estrutura Física

- Switches gerenciáveis;
- Placa de rede padrão Ethernet;
- Cabeamento estruturado Cat 5e;
- Sistema de monitoramento de vídeo/TV;
- Sistema de controle de acesso aos blocos por cartão.

3.2.1.6 Estrutura Lógica

- Endereçamento classe B (150.162.xxx.xxx);
- Protocolo Ethernet: IEE 802.3u, IEE 802.3ab e IEE 802.3z;
- Serviços: HTTP, HTTPS, WWW, FTP, SMTP, POP3, SNMP, VoIP, Servidor de arquivo e impressão;
- Sistema de suporte: helpdesk do NPD e do NDA;
- Recuperação de falhas;
- Software setorial: Windows XP, Ubuntu Linux, CFX, Office windows, BrOffice.org, CFX, Matlab, Adobe Acrobat;
- Atualizações.

3.2.2 Pontos Fracos

3.2.2.1 Aspectos Culturais / Comportamentais

Por ser uma repartição pública, onde os funcionários são regidos pelo RJU, é um fator complicador fazer com que respeitem a política de segurança na sua integralidade.

3.2.2.2 Fontes de Poder e Política da Informação

O cargo de Chefe Departamental tem uma influência parcial, já que não tem o poder de demitir.

3.2.2.3 Processos de Gerenciamento da Informação

É complicado a sua operacionalização no ambiente organizacional de um Departamento.

3.2.2.4 Equipes de Profissionais

Há necessidade que a organização tenha um Comitê de Segurança da Informação vigente e atuante.

3.2.2.5 Estrutura Física

O Departamento necessita adequar a sua tecnologia de informação às normas e padrões existentes. O exemplo mais evidente está no fato do EQA não possuir um sistema de cabeamento estruturado.

Os racks que comportam os switches deveriam ser fechados para impossibilitar a conexão não autorizada de um computador às portas do switch.

As tomadas de rede, localizadas nas paredes, deveriam possibilitar o acesso à internet somente com autorização do administrador, através de controle por endereço MAC.

3.2.2.6 Estrutura Lógica

Recuperações de falhas: não possui.

Atualização: devido ao fato da maioria dos programas não ser licenciados, não possibilita atualização.

3.3 SITUAÇÃO ATUAL

Em visitas realizadas ao EQA, os autores identificaram algumas vulnerabilidades. Abaixo elencamos as que devem ser consideras com maior relevância:

- **Ausência de servidor de arquivos**: Com a ausência de um servidor para concentrar os arquivos gerados pelo departamento, as informações estão guardadas em vários equipamentos o que dificulta a administração e as cópias de segurança;

- **Ausência de servidor de backup**: Além da ausência de um servidor para a concentração de informações, o Departamento também necessita de um servidor de backup. Esta deficiência gera desconformidade em relação à salva-guarda da informação e da retirada da cópia do local de origem em dispositivo distinto, conforme itens 10.5 à 10.7 da ABNT NBR ISO/IEC 17799:2005;
- **Ausência de autenticação de usuários na rede**: Constatou-se ausência na identificação dos usuários que acessam os recursos da rede do Departamento, dificultando assim o gerenciamento dos acessos lógicos, item 11.5.2 da ABNT NBR ISO/IEC 17799:2005;
- **Sistemas operacionais sem licenciamento**: Foram detectadas estações de trabalho com sistemas operacionais sem licenciamento e consequente falta de atualização adequada, o que compromete a segurança da rede;
- **Aplicativos sem licenciamento**: Foram detectadas estações de trabalho com aplicativos sem licenciamento e consequente falta de atualização adequada, o que compromete a segurança da rede;
- **Cabeamento não estruturado, com pontos de rede expostos**: O cabeamento da rede lógica não é estruturado e possui inúmeros itens desconformes em relação a acessos lógicos e físicos, além da falta de documentação. Existem cabos de rede UTP, indicados para utilização interna, expostos ao tempo e ao ataque físico. A Figura 3-1 apresenta um exemplo de cabos UTP expostos ao tempo e a ataques físicos;

Figura 3-1: Cabeamento externo exposto ao tempo e ataques físicos

- **Distribuição irregular de ativos na rede**: Alguns hubs e switches não gerenciáveis (Figura 3-2) estão distribuídos pela rede sem controle, aumentando assim os pontos de falha e acessos físicos indevidos à rede;

Figura 3-2: Switch não gerenciável instalado de forma irregular

- **Estrutura de madeira**: Alguns blocos do EQA possuem construção em madeira, nos quais existe a acomodação de equipamentos e instalações

elétricas antigas, e fogareiros para experiências químicas, o que aumenta o risco de incêndio no local;

Figura 3-3: Edificação com estrutura de madeira

- **Endereços IP públicos nas estações de trabalho**: Foi constatado que todos os equipamentos da rede do EQA estão configurados com endereçamento IP público, o que expõe a rede à ataques oriundos principalmente da Internet;
- **Falta de controle de acesso físico**: Contrariando a ABNT NBR ISO/IEC 17799:2005, não há política regulamentar sobre o acesso físico. A Figura 3-4 apresenta o exemplo de cartão magnético de acesso, sem foto ou identificação do usuário. O claviculário geral é acessado por funcionário da UFSC e funcionários de empresas terceirizadas, dando acesso à todas as dependências do Departamento, com exceção a alguns laboratórios, que possuem acesso por autenticação;

Figura 3-4: Falta de controle o acesso físico

- **Impressoras expostas**: Existem impressoras instaladas em vários corredores onde o material impresso pode sofrer um ataque indevido. Além disso, o ponto de rede que alimenta a impressora pode ser facilmente utilizado para acesso à rede, através de equipamento portátil, conforme pode ser verificado na Figura 3-5;

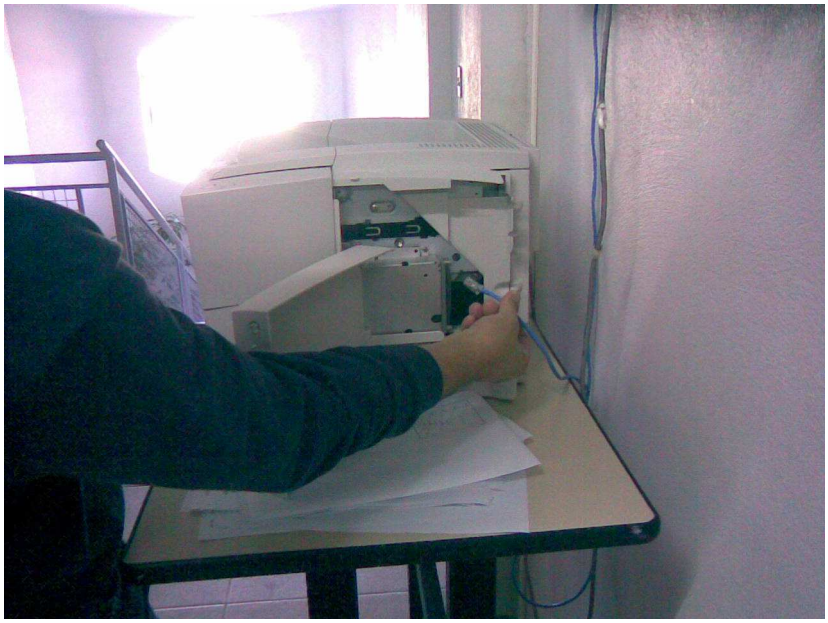


Figura 3-5: Ponto de rede da impressora sem proteção e em local público

- **Energia elétrica**: Não há tratamento quanto a minimizar os impactos da falta de energia elétrica. Há ausência de no-breaks e grupos geradores. Também não há redundância na alimentação da energia. Há casos em que o cabeamento elétrico (preto) compartilha o mesmo duto ou há cruzamento com o cabeamento lógico (azul), o que pode ocasionar curto circuito ou interferência eletromagnética, conforme pode ser verificado na Figura 3-6;

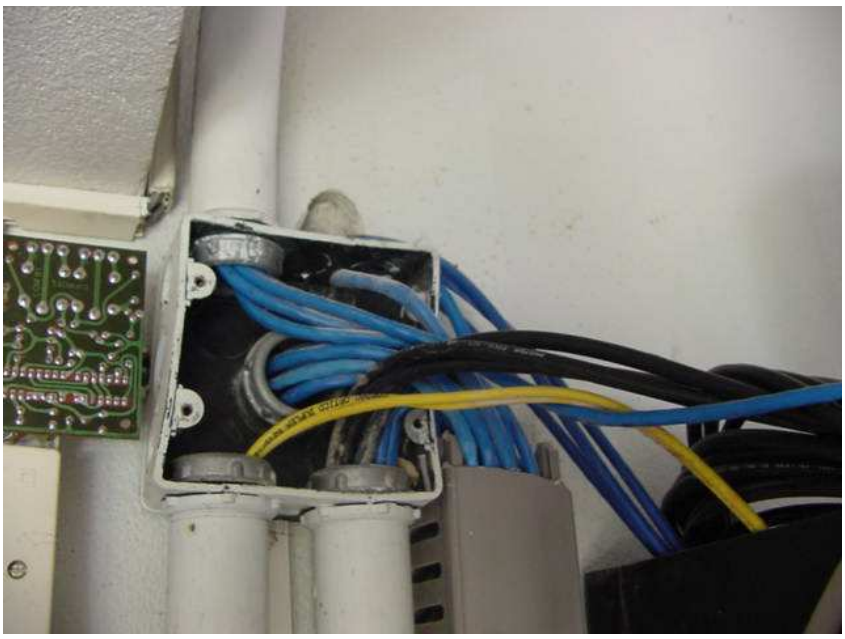


Figura 3-6: Exemplo de instalação incorreta de cabeamento elétrico e de dados

- **Utilização indevida de access points**: Constatou-se a utilização de access points através de senhas compartilhadas. Este tipo de prática contraria o item 10.6.2 da ABNT NBR ISO/IEC 17799:2005;

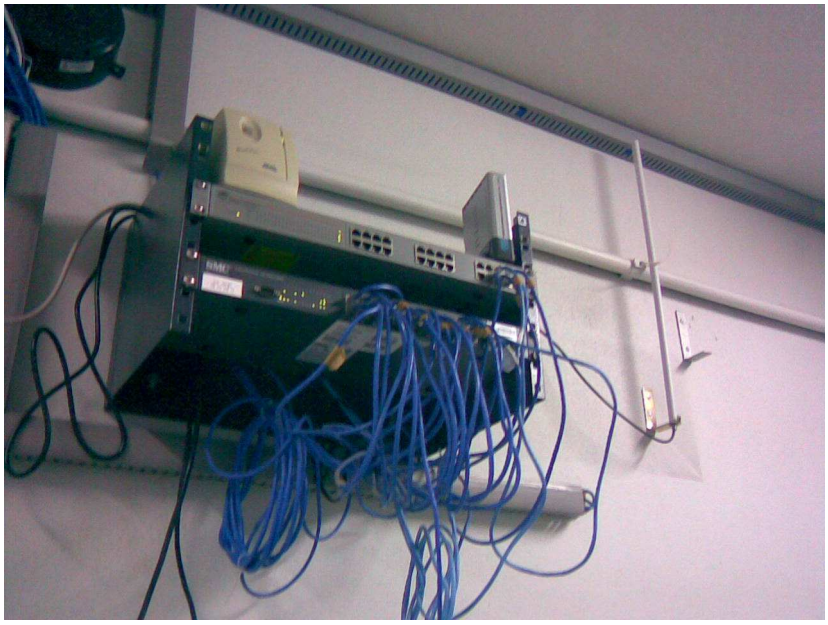


Figura 3-7: Exemplo de um dos access points irregulares

- **Não há política para navegação**: Não existe controle para o serviço de navegação na internet;
- **Não há política para utilização de e-mail**: Não existe controle para o serviço de correio eletrônico;
- **Há uma política de uso aceitável**: Existe uma política de uso aceitável, que está sendo levada em consideração para a construção deste plano de segurança, mas insuficiente como política de segurança;
- **Acesso à BIOS dos desktops sem senha**: As interfaces USB das estações de trabalho estão habilitadas para receber qualquer tipo de dispositivo, o que aumenta as vulnerabilidades da rede.

4 ESTRATÉGIAS DE SEGURANÇA DAS INFORMAÇÕES

4.1 ETAPA CONCEITUAL

4.1.1 Classificação da Informação

A Classificação da Informação ajuda a definir níveis e critérios adequados de proteção das informações, garantindo a confidencialidade, conforme a importância da organização.

As informações, tanto em meio físico quanto eletrônico, possuem necessidades de proteção quanto a confidencialidade, integridade e disponibilidade, bem como quaisquer outros requisitos que sejam necessários. Em geral, a classificação dada à informação é uma maneira de determinar como esta informação será tratada e protegida.

A Lei 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências, estabelece no Capítulo I, que trata das disposições gerais, que “é dever do Poder Público a gestão documental e a proteção especial a documentos e arquivos, como instrumento de apoio à administração, à cultura, ao desenvolvimento científico e como elemento de prova e informação”. A mesma Lei define que “arquivo” é “o conjunto de documentos produzidos e recebidos por órgãos públicos, instituições de caráter público e entidades privadas, em decorrência do exercício de atividades específicas”, perfil que se enquadra o EQA. Considera também que a “gestão de documentos é o conjunto de procedimentos e operações técnicas à sua produção, tramitação, uso, avaliação e arquivamento em fase corrente e intermediária, visando a sua eliminação ou recolhimento para guarda permanente”.

Respaldada nesta Lei a UFSC publicou em 1995 (em papel) e re-editou em 2009 (na Internet), a Tabela de Temporalidade (DMSG, 2009) que, entre outros objetivos, classifica a informação, destaca a importância da vida útil dos documentos nos meios acadêmicos e administrativos, fixa prazos de permanência em cada órgão e define a destinação final de cada documento. Conforme o Dicionário de Terminologia Arquivística, (2005, p. 159), é o instrumento de destinação, aprovado

por autoridade competente, que determina prazos e condições de guarda tendo em vista a transferência, recolhimento, descarte ou eliminação de documento.

Conforme disposto no Artigo 5, do Decreto 4.553, de 27 de dezembro de 2002, da Casa Civil, que regula o Artigo 23, da Lei 8.159, “os dados ou informações sigilosos serão classificados em ultra-secretos, secretos, confidenciais e reservados, em razão do seu teor ou dos seus elementos intrínsecos”. A redação completa da classificação dos documentos é a seguinte:

§ 1° São passíveis de classificação como ultra-secretos, dentre outros, dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.

§ 2° São passíveis de classificação como secretos, dentre outros, dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

§ 3° São passíveis de classificação como confidenciais dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.

§ 4° São passíveis de classificação como reservados dados ou informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Conforme disposto no Artigo 7 do mesmo Decreto, foram definidos os prazos de duração da classificação e que passam a vigorar a partir da data de produção do dado ou informação e são os seguintes:

a) **Ultra-secreto:** máximo de trinta anos;
b) **Secreto:** máximo de vinte anos;
c) **Confidencial:** máximo de dez anos;
d) **Reservado:** máximo de cinco anos.

Analisando a Tabela de Temporalidade, verifica-se que, em função dos prazos definidos para os documentos, em especial os do EQA têm classificação máxima de “reservado” e que, desde que não tenham a classificação renovada, são encaminhados ao Arquivo Central após, no máximo, cinco anos.

4.1.2 Análise de Risco

Riscos existem em qualquer atividade e não são apenas relacionadas à tecnologia. Na maioria das atividades os riscos podem ser financeiros, contábeis, legais, ambientais, humanos, entre outros.

Os riscos relacionados com a segurança da informação podem ser de diversos tipos, tais como danos físicos, erro humano, mau funcionamento de equipamentos ou sistemas, ataques internos ou externos, uso inadequado dos dados ou a perda destes.

A análise de riscos é uma das ferramentas da gestão de riscos e serve como um método de identificação destes riscos, além de determinar salvaguardas adequadas, objetivando a correta aplicação de recursos na redução destes riscos.

> Os requisitos de segurança da informação são identificados por meio de uma análise/avaliação sistemática dos riscos de segurança da informação. Os gastos com os controles precisam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança da informação.
> Os resultados da análise/avaliação de riscos ajudarão a direcionar e a determinar as ações gerenciais apropriadas e as prioridades para o gerenciamento dos riscos da segurança da informação, e para a implementação dos controles selecionados para a proteção contra estes riscos. (ABNT, 2005).

A análise de risco desenvolvida para este plano estratégico está disponível no Apêndice I.

4.1.3 Políticas de Segurança

O objetivo da política de segurança da informação, segundo (ABNT, 2005), é “prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes”.

> A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações.
> Seu desenvolvimento é o primeiro e o principal passo da estratégia de segurança das organizações. É por meio dessa política que todos os aspectos envolvidos na proteção dos recursos existentes são definidos e, portanto, grande parte do trabalho é dedicado à sua elaboração e ao seu planejamento (NAKAMURA, 2003).

Uma proposta de política de segurança, desenvolvida para este plano estratégico, está disponível no Apêndice II.

4.1.4 Direito de Acesso

A política de direito de acesso será abordado no item 4.3 Acessos Lógicos e Físicos.

4.2 ADMINISTRAÇÃO DE SEGURANÇA

4.2.1 Tipo de Estrutura

A UFSC é uma estrutura acadêmico-administrativa composta por diversas estruturas menores da mesma natureza. Cada estrutura-filha tem um organograma próprio, independente e sustentável, mas ao mesmo tempo dependente da estrutura principal.

Para (CARUSO, 1999) a estrutura de administração da segurança pode ser de dois tipos: centralizada e descentralizada. Cada uma tem sua característica peculiar:

> Segurança centralizada: proporciona controle mais eficiente com relação a mudanças na segurança e possivelmente nos esforços para se impor a segurança. Mas o esforço de manutenção da segurança neste nível pode requerer o gerenciamento de uma equipe considerável;
> Segurança descentralizada: distribui o esforço de manutenção da segurança, de maneira que a função não se torne um ônus para uma única área. Além disso, a manutenção poderá ser subordinada a uma área que pode ter um conhecimento maior e mais adequado dos recursos a ser protegidos. Entretanto, haverá um esforço adicional na área central para controlar as atividades dos administradores descentralizados (CARUSO, 1999).

No caso do EQA, para que a administração de segurança das informações ali produzidas possa contar com uma estrutura que contenha a maioria das vantagens dos dois tipos, ela deveria ser centralizada e descentralizada, ou seja, enquanto pertencente ao organograma do EQA, seria centralizada, mas seria descentralizada da administração principal, localizada no NPD.

4.2.2 Localização Dentro da Estrutura

A administração da segurança é uma área que, por sua natureza e importância, deverá se relacionar “mais diretamente com a alta administração” (CARUSO, 1999) da estrutura a qual estiver subordinada. Isto se torna necessário para que se torne menos suscetível a pressões e comportamentos resultantes de lealdades para com a área funcional à qual pertença.

4.2.3 Perfil do Profissional

O perfil do profissional de segurança deve ser cuidadosamente definido, pois o trabalho que exercerá é difícil e exigirá que conheça todos os detalhes da organização. É uma atividade que requer “alta responsabilidade, segurança nas ações e decisões e determinação” (CARUSO, 1999), além de:

- Conhecimento dos recursos dos ambientes de informações;
- Conhecimento dos requisitos de segurança adequados;
- Alto grau de responsabilidade;
- Boa experiência analítica e organizacional;

- Sensibilidade para a política do ambiente de informações;
- Facilidade nos relacionamentos pessoais;
- Estabilidade emocional.

4.2.4 Diretrizes de Segurança

O EQA já dispõe de diretrizes de segurança, que são os procedimentos básicos que cada usuário da rede deve seguir.

Estas diretrizes são regras simples e de fácil entendimento, denominada “Política de Uso Aceitável”.

4.2.5 Ferramentas Administrativas e Técnicas

A avaliação da ferramenta de segurança é uma tarefa para a equipe do projeto e não de uma área específica.

4.2.6 Equipe do Projeto

Equipe do projeto:

- Comissão de estudo e elaboração do planejamento e implantação da estrutura global da segurança;
- Equipe que vai desenvolver o projeto da implantação da segurança;
- Composta por elementos das diversas áreas envolvidas ou relacionadas diretamente com as atividades de processamento de informações;
- Quantidade de componentes restrita, mas compatível com o tamanho da organização e, variedade, quantidade e porte dos equipamentos;
- Perfil profissional variado;
- Caso a equipe seja grande, as tarefas devem ser divididas em função das especializações dos membros;
- Dedicam parte de seu tempo para o projeto;

- Não deve se envolver com as tarefas relacionadas com a operacionalização da segurança;
- Não deve ser confundida com a equipe de administração de segurança.

A Equipe do projeto (Figura 4-1) deverá ser composta com elementos das seguintes áreas:

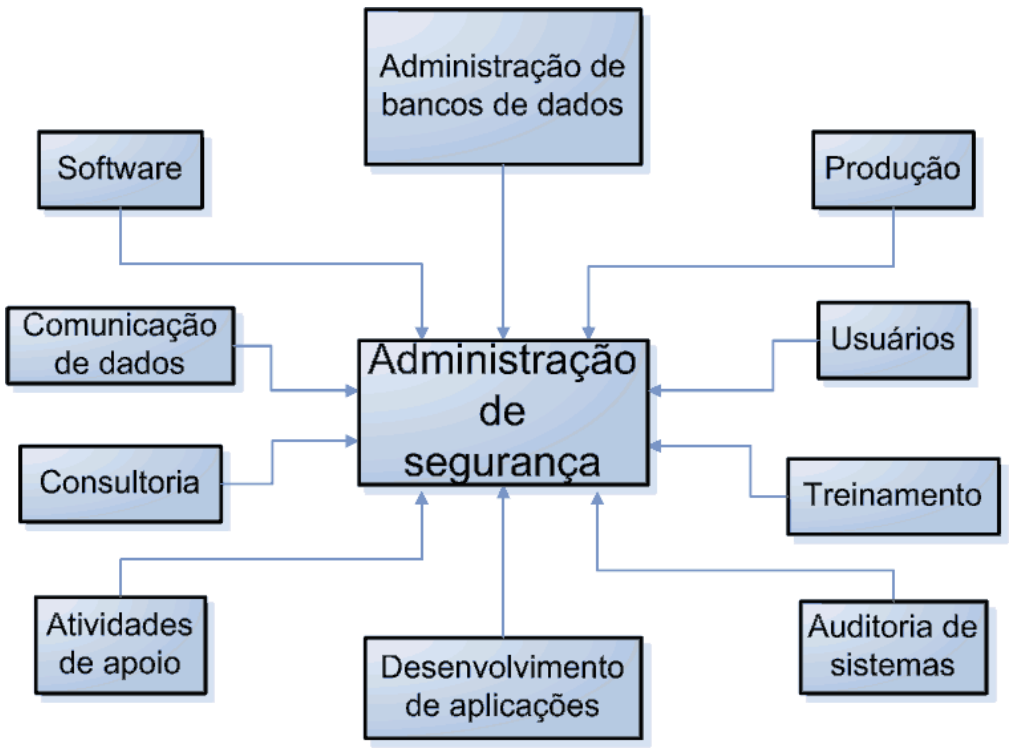


Figura 4-1: Modelo de estrutura de equipe de projeto de segurança

- Administração de segurança:
  - Tem a função de coordenar o projeto;
  - Pode ser assessorado por outros membros da equipe de segurança para a execução das tarefas operacionais exigidas pela implantação.
- Software básico e de apoio:
  - Responsável técnica pelo ferramental de informática utilizado para processar e armazenar informações;
  - Caberá a implantação da ferramenta de segurança e sua adaptação ao ambiente operacional da organização;
  - Faz uso de recursos que contornam a segurança ou propiciam o desenvolvimento de brechas na segurança;

  - Define diretrizes básicas de informática e de processamento de informações;
  - Pode absorver a função de administrar o banco de dados.
- Administração de dados:
  - Responsável pela:
    - Administração dos ativos de informação residentes nos computadores;
    - Operacionalização e uso dos softwares de banco de dados;
    - Integridade dos ativos de informação residentes em banco de dados;
    - Norma de nomes de arquivos.
- Produção:
  - Responsável pelo processamento de todos os serviços de informática;
  - Está em contato mais direto com os usuários;
  - Será afetada pelas medidas de segurança, caso tenha que administrar os requisitos de segurança de acesso de usuários aos computadores;
  - Custodiante dos ativos de informação, portanto, a mais interessada na preservação da integridade dos ativos sobre os quais tem responsabilidade.
- Comunicação de dados e redes:
  - Responsável pela manutenção e disponibilidade das linhas de comunicação e ativos relacionados;
  - Possui requisitos de segurança próprios e específicos;
  - Deve possuir profundos conhecimentos dos protocolos de comunicação para internet e intranet, além das ferramentas relacionadas.
- Desenvolvimento de aplicações:
  - Responsável pelo desenvolvimento de aplicações para as áreas da organização que não tenham estrutura de possuir uma área de desenvolvimento autônoma;

  - Responsável pelos recursos de desenvolvimento de aplicações (bibliotecas de linguagens, ferramentas e normatização);
  - Responsável por estabelecer um padrão único de segurança de aplicativos.
- Auditoria:
  - Controla o uso dos ativos da organização em nome dos legítimos proprietários, através da adesão das partes às normas e procedimentos estabelecidos;
  - Deve garantir que o processo de implantação de segurança e as próprias diretrizes de segurança sigam as diretrizes globais da organização.
- Usuários:
  - Pode ser um representante legítimo dos usuários ou uma comissão composta por um membro de cada área da organização;
  - Participará nas decisões de todas as medidas que impliquem na participação de usuários;
  - Será consultado nos assuntos que envolvam necessidades específicas dos usuários.
- Treinamento:
  - Responsável pelas atividades de treinamento, relacionadas com os requisitos de segurança, para novos funcionários e a atualização dos já existentes;
  - A estrutura de treinamento deverá permanecer após o encerramento do projeto.
- Atividades de apoio:
  - Responsável pelas atividades extras, que não estejam relacionadas diretamente com informações, tais como:
    - Administração patrimonial;
    - Transportes;
    - Comunicações;
    - Outras.
  - Deve fornecer consultoria, apoio técnico e administrativo relacionados com suas áreas de conhecimento.

- Consultoria externa:
  - Dos fornecedores dos equipamentos;
  - Dos fornecedores de ferramentas de segurança;
  - De consultores de segurança.

Equipe de Administração de segurança:

- Devem ser alocados nas tarefas operacionais decorrentes da própria administração de segurança;
- Responsável pela operacionalização das medidas propostas pela equipe do projeto.

4.3 ACESSOS LÓGICOS E FÍSICOS

Foram encontradas vulnerabilidades nos acessos lógicos e físicos ao EQA, conforme o item 3 ANÁLISE. A seguir abordaremos os principais tópicos que serão tratados.

4.3.1 Nível de Permissão e Classificação de Usuários

Na Tabela 4-1 são apresentados os níveis de permissão e classificação dos usuários.

Tabela 4-1: Níveis de permissão e classificação dos usuários.

Tipo de usuário	Descrição	A quem se aplica
Administrador domínio	Permissão de acesso total aos servidores e estações para administração de recursos e políticas do domínio	Membro do corpo técnico/administrativo, responsável pela administração da rede
Administrador estação de trabalho	Permissão de acesso total às estações de trabalho para administração de recursos e políticas	Membro do corpo técnico/administrativo responsável pela administração das estações de trabalho
Administrador Local Servidor	Permissão de acesso total somente ao servidor sem propriedades de	Membro do corpo técnico/administrativo

Tipo de usuário	Descrição	A quem se aplica
	administração de domínio	responsável pela administração do servidor
Usuário de domínio	Permissão de acesso às estações de trabalho conforme pré-definido pelas políticas elaboradas no servidor de domínio e pelas necessidades de acesso aos aplicativos locais	Corpo discente, corpo docente e corpo técnico/administrativo
Usuário estação de trabalho	Direito de acesso à estação de trabalho onde o usuário estiver sido criado, com condições locais de acesso	Corpo discente, corpo docente e corpo técnico/administrativo

4.3.2 Sistemas Operacionais

Na Tabela 4-2 são apresentados os sistemas operacionais utilizados.

Tabela 4-2: Sistemas operacionais utilizados.

Sistema	Permissões Aplicáveis
Microsoft Windows XP	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Ubuntu Linux	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Microsoft Windows 2003 Server	Administrador de domínio
	Administrador local servidor
Open SUSE Linux	Administrador de domínio
	Administrador local servidor

4.3.3 Aplicativos

Na Tabela 4-3 são apresentados os aplicativos utilizados.

Tabela 4-3: Aplicativos

Sistema	Permissões Aplicáveis
Microsoft Office	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
BrOffice.org	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Matlab	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Adobe Acrobat Writer 5.0	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Adobe Acrobat Reader	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Matemática	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Estatística	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
CFX	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Autocad	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
Pró-engineer	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho
F-secure	Administrador Domínio
	Usuários do domínio
	Administrador estação de trabalho

4.3.4 Criptografia de Comunicação

- É recomendada a utilização de criptografia nos notebooks utilizados nas pesquisas, buscando aumentar a confidencialidade dos documentos;
- É recomendada a criptografia na rede por onde trafegam os dados de registro de pesquisas no software que gerencia os projetos de pesquisa.

4.3.5 Segurança das Estações e Notebooks

- **Antivírus:** Utilizar antivírus corporativo e de administração centralizada;
- **Criptografia:** É recomendada a utilização de criptografia nas estações utilizadas nas pesquisas, buscando aumentar a confidencialidade dos documentos;
- **Atualizações do sistema operacional:** Administração dos sistemas operacionais deve ser administrada centralizadamente e de forma automatizada, de modo a proporcionar um nível máximo de atualização;
- **Bloqueio da estação em inatividade:** A administração da rede deve promover o bloqueio da estação de trabalho após um curto espaço de tempo de inatividade;
- **Atualizações de aplicativos:** Os aplicativos que serão utilizados nas estações devem ser previamente homologados e instalados somente pela administração da rede. Sendo permitida a utilização somente de software licenciado ou livre;
- **Controle de patrimônio:** Um inventário de hardware e software deve ser implementado para auxiliar no controle do hardware e do software das estações.

4.3.6 Segurança da Rede

- A rede atual já é monitorada através de sensores que detectam anomalias na rede, através do NPD da UFSC;
- Apesar do trabalho não focar especificamente a segurança da rede,

recomenda-se que seja implementada NAT, nas redes do EQA, visando à retirada de endereços IP públicos nas estações de trabalho. A Figura 4-2 modela a topologia da rede conforme proposta;

- Servidor Radius: Implementação de um servidor Radius para limitar e regular as conexões à rede do departamento;
- Servidor de domínio: Implementação de servidor de domínio no departamento, buscando a autenticação dos usuários na rede e conseqüente diminuição do não repúdio;
- Servidor de Arquivos: Implementação de um servidor de arquivos, com permissões pré-definidas pelo servidor de autenticação;
- Servidor de Backup: Implementação de servidor de backup para o departamento através da utilização de mídias removíveis e/ou espelhamento de arquivos e aplicação em outra unidade da UFSC;
- Revisar o cabeamento de rede no intuito de estruturá-lo e documentá-lo, diminuindo assim os pontos de rede em exposição;
- Nas redes do EQA deve-se inibir na camada de rede a utilização dos compartilhamentos de pastas não autorizados entre estações de trabalho, notebooks e similares.

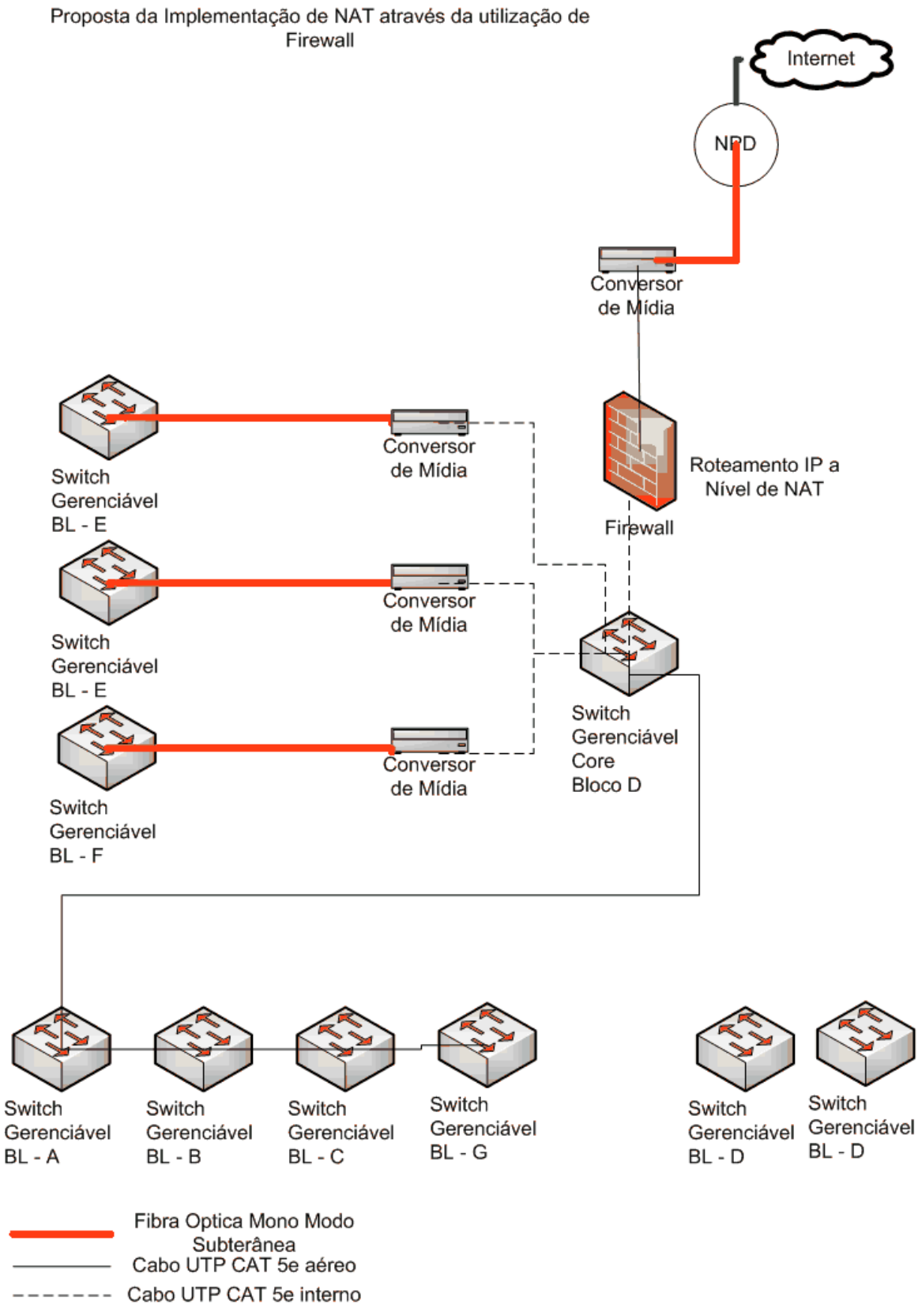


Figura 4-2: Topologia da rede utilizando NAT

4.3.7 Procedimento Operacional de Segurança Física

- Obrigatoriedade para o uso do crachá de identificação;
- Implementar níveis de acesso físico às dependências do departamento;
- Eliminar edificações em madeira;
- Estrutura da sala cofre conforme norma, incluindo ar-condicionado redundante, sensor de fumaça, sensor de temperatura, tranca eletrônica com log de acesso, fornecimento de energia elétrica compatível com o ambiente;
- Implementar controle de acesso físico à sala do backbone e servidores do EQA, para funcionários e terceirizados, através de controle eletrônico de senhas;
- Utilizar termo de responsabilidade e confidencialidade junto aos funcionários e terceirizados.

4.3.8 Segurança dos Meios de Armazenamento

- Criptografar todas as mídias que armazenarem pesquisas classificadas como de suma importância;
- Elaborar política de descarte de mídia para minimizar o risco de vazamento de informações;
- Os dispositivos com mídias de armazenamento de relativa importância devem estar alocados em áreas de acesso restrito e controles adicionais, como a sala cofre.

4.4 ANÁLISE DA VIABILIDADE ECONÔMICO / FINANCEIRA

Baseado no plano estratégico proposto, foi desenvolvido uma tabela de orçamento dos custos (Tabela 4-4) na qual consta a estimativa de valores para implantação do projeto, com as respectivas rubricas.

Assim sendo, foram apresentadas duas propostas:

a) **Orçamento de Requisito Técnico ideal (Orçamento Ideal):** Requisitos técnicos para que o EQA tenha um padrão ideal de segurança da informação e da infraestrutura de TI;
b) **Orçamento de Requisito Técnico Mínimo (Orçamento Mínimo):** Requisitos técnicos para que o projeto tenha um padrão mínimo aceitável de segurança, enquanto o orçamento para a situação ideal não é liberado.

Tabela 4-4: Orçamento para implantação do projeto

Rubrica	Descrição	Orçamento Ideal (R$)	Orçamento Mínimo (R$)
Hardware			
34490.52.35	Firewall	15.000,00	15.000,00
34490.52.35	Access point	3.000,00	600,00
34490.52.35	Switch	15.000,00	
34490.52.35	No-break	8.000,00	2.000,00
34490.52.35	Gerador de energia	-	-
34490.52.35	Material para cabeamento estruturado	50.000,00	-
34490.52.35	Patch panel Cat 5e	5.000,00	-
34490.52.35	Servidor	30.000,00	30.000,00
Serviços			
3339.36.06	Mão-de-obra cabeamento estruturado	20.000,00	-
33390.39.95	Manutenção de equipamentos	15.000,00	-
3339.36.06	Consultoria em segurança	35.000,00	-
33390.39.08	Consultoria implementação S.O.	20.000,00	-
	Treinamentos	-	15.000,00
Software			
33390.30.47	Software - S.O.	10.000,00	10.000,00
33390.39.01	Software - Antivírus	40.000,00	-
33390.39.01	Software - Criptografia	-	-
33390.39.01	Software - Pacote Office	-	-
Total		**266.000,00**	**72.600,00**

Para auxiliar a análise da viabilidade econômica e financeira do projeto foi utilizada a Tabela 4-5 demonstrando os seguintes valores:

Tabela 4-5: Análise da viabilidade econômica / financeira

Orçamento do Projeto		Orçamento 2009		
		UFSC	UFSC (TI)	EQA
		1.220.231.946,00	730.000,00	100.000,00
Ideal	266.000,00	0,02%	36,44%	266,00%
Mínimo	72.600,00	0,01%	9,95%	72,60%

Constatou-se que:

a) O orçamento destinado ao EQA, para a área de TI, é baixo diante das necessidades do projeto;
b) O valor do Orçamento Mínimo representa 72,6% do orçamento do EQA, 9,95% do orçamento destinado às Ações de Informática da UFSC e apenas 0,01% do orçamento total da UFSC, todos para 2009, e poderia ser implementado em até dois anos;
c) O valor do Orçamento Ideal representa 266% do orçamento do EQA para 2009, o que o torna inviável para este ano, mas por representar, 36,44% do orçamento das Ações de Informática da UFSC, e apenas 0,02% do orçamento total, caberia o estudo de suplementação da verba orçamentária, em TI, para o EQA;

Quanto ao ROI, por se tratar de uma instituição de ensino superior federal, que não visa lucro e sim o desenvolvimento acadêmico e a produção de patentes, o que deve ser enfatizado é a questão da segurança dos projetos e da imagem da instituição, caso ocorra perda ou vazamento de dados sigilosos ou sensíveis. Analisando por este ponto de vista o valor do Orçamento Ideal será baixo, diante das perdas potenciais.

5 PLANOS DE SEGURANÇA

5.1 MONITORAMENTO E CONTROLE

O item 5 do Apêndice I apresenta os procedimentos de monitoramento e controle para cada evento de risco previsto no EQA e que podem comprometer a segurança das informações existentes no Departamento.

5.2 RESPOSTA EMERGENCIAL

O item 5 do Apêndice I apresenta os procedimentos que serão aplicados, no caso de uma resposta emergencial, a um dos eventos de risco previstos.

5.3 PLANO DE CONTINGÊNCIA

O plano de contingência para o EQA está descrito em detalhes no Apêndice III.

6 CONSIDERAÇÕES FINAIS

6.1 CONCLUSÃO

Antes de iniciar este trabalho, sabia-se que seriam muitas as dificuldades e limitações na obtenção de informações para o desenvolvimento deste plano estratégico, as quais foram confirmadas. Para transpô-las foi necessário planejar e executar cuidadosamente todas as etapas que seriam executadas a seguir, para que o objetivo geral e específico pudesse ser alcançado.

O primeiro passo foi a análise geral das atividades do EQA para determinar qual seria o foco e o escopo deste trabalho. Em seguida foram realizadas vistorias ao ambiente do Departamento para captar todas as nuances das vulnerabilidades existentes. Os principais problemas foram registrados e fotografados para servirem de material de análise do ambiente. Nesta etapa concluiu-se que os principais ativos de informação que deveriam ter um plano estratégico de segurança da informação seriam os trabalhos acadêmicos e pesquisas, cujos resultados poderiam se transformar em patentes desenvolvidas pela UFSC e que recebem patrocínio externo.

O segundo passo foi o levantamento documental a partir de diversas fontes, tais como normas, legislação (federal, estadual e municipal), documentos internos e entrevistas com servidores da instituição. No caso destes últimos a obtenção das

informações que seriam relevantes ao trabalho teve de ser cuidadosa, para que fosse extraído apenas o conhecimento tácito que respondesse aos questionamentos pertinentes ao planejamento, sem expor dados confidenciais que comprometessem ainda mais a segurança do Departamento ou da Universidade.

De posse deste material restou apenas montar o “quebra-cabeça” que se formou o que exigiu algumas semanas de análises e discussões.

O resultado final, sintetizado neste trabalho, confirmou a necessidade do EQA em implantar um plano estratégico de segurança da informação. Ficou evidente que o principal obstáculo é a cultura interna, resistente às regras ou limitações, característica de um ambiente acadêmico e, principalmente, estatutário. Apesar de ser um fator de uma solução complexa é possível de ser solucionado, através da mudança da cultura e do comportamento dos envolvidos.

6.2 LIMITAÇÔES

Além do fator humano o EQA também tem carência em soluções de tecnologia da informação, desde a aquisição de hardware e software, passando pela definição e implantação de política de segurança, direitos de acesso e planos de continuidade do negócio e de contingência. São tarefas complexas que requererão dedicação das equipes envolvidas no processo.

Para completar o quadro existe a limitação orçamentária, que por ser insuficiente para as necessidades apresentadas, impede a implementação do plano, na sua totalidade, em curto prazo. A solução neste caso, que passa pela revisão e ampliação do orçamento do EQA, exigirá diversas etapas burocráticas através dos diversos órgãos reguladores. Entretanto, como forma alternativa, existe a possibilidade de implementação parcial do plano, enquanto o restante do orçamento é pleiteado.

6.3 TRABALHOS FUTUROS

Em relação a trabalhos futuros este Plano de Segurança da Informação, oferece algumas opções no que diz respeito a continuidade do desenvolvimento do plano estratégico de segurança da informação do EQA. Abaixo são citadas algumas:

- **Infraestrutura de rede:** Para que sejam eliminadas as vulnerabilidades de disponibilidade da rede se faz necessário um plano de reestruturação da rede física, transformando a rede existente numa estrutura que utilize cabeamento estruturado na plenitude da norma EIA/TIA-568-B.1-2001;
- **Segurança de rede:** Neste trabalho foi constatada a utilização maciça de endereços públicos na maioria dos hosts, tanto do EQA quanto da UFSC. Esta característica expõe toda a rede a ataques externos e se contrapõe às técnicas existentes de ocultação e proteção de hosts sensíveis. Neste caso cabe um estudo para implantação de NAT e DMZ.

REFERÊNCIAS

ABNT. (Brasil). **Tecnologia da Informação – Código de prática para a gestão da segurança da informação** – NBR ISO/IEC 17799:2005. Rio de Janeiro, 2005. 52 p.

CAPES. **Tabela Grande Área da Engenharia Química.** Santa Catarina, Nov 2009. Disponível em: http://conteudoweb.capes.gov.br/conteudoweb/ProjetoRelacaoCursosServlet?acao=pesquisarGrandeArea. Acesso em 01 nov. 2009.

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações.** 2ª ed. rev. e ampl. São Paulo: Editora SENAC São Paulo, 1999. 367 p.

CERT.br. **Cartilha de Segurança para Internet.** Versão 3.1/CERT.br. São Paulo: Comitê Gestor da Internet no Brasil, 2006. ISBN: 978-85-60062-06-5. ISBN: 85-60062-06-8.

COPERVE. **Relatório oficial Vestibular UFSC/2009.** Santa Catarina: COPERVE, 2009. Disponível em: http://www.vestibular2009.ufsc.br/resultado/resultadoOficialV2009.pdf. Acesso em: 01 nov. 2009. 340 p.

CPGEA. **Linhas de pesquisa.** Santa Catarina, nov. 2009. Disponível em: http://www.enq.ufsc.br/pgrad/cpgea/padrao.php?link=linhas_pesquisas. Acesso em: 02 nov. 2009.

CPGENQ. **Linhas de pesquisa.** Santa Catarina, nov. 2009. Disponível em: http://www.cpgenq.ufsc.br/port/linhas_pesquisa.html. Acesso em: 02 nov. 2009.

DIT. **Departamento de Inovação Tecnológica.** Santa Catarina, out. 2009. Disponível em: http://www.dit.ufsc.br. Acesso em: 01 out. 2009.

DMSG. **Tabela de temporalidade.** Santa Catarina, nov. 2009. Disponível em: http://notes.ufsc.br/aplic/temporalidade.nsf. Acesso em: 16 nov. 2009.

DSIC. **Departamento de Segurança da Informação e Comunicações.** Distrito Federal, out. 2009. Disponível em: http://dsic.planalto.gov.br. Acesso em 01 out. 2009.

EQA. **Departamento de Engenharia Química e Engenharia de Alimentos.** Santa Catarina, out. 2009. Disponível em: http://www.enq.ufsc.br. Acesso em: 01 out. 2009.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação.** Rio de Janeiro: Editora Ciência Moderna Ltda., 2003. 162 p. ISBN: 85-7393-290-2.

GLASER, Barney G.; STRAUSS, Anselm L. **The Discovery of Grounded Theory: Strategies for Qualitative Research.** Chicago: Aldine de Gruyter, 1967.

GONÇALVES, Luis Rodrigo de Oliveira. **Pequeno histórico sobre o surgimento das Normas de Segurança.** Disponível em: http://www.lockabit.coppe.ufrj.br/print.php?id=69. Acesso em: 08 mar. 2006.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de metodologia científica.** 6ª ed. - 7ª reimpr. – São Paulo: Atlas. 2009. 315 p.

MERRIAM, Sharan B. **Qualitative research and case study applications in education.** San Francisco: Jossey-Bass, 1998.

MICROSOFT BRASIL. Academia Latino-Americana de Segurança da Informação. **Introdução à ABNT NBR ISO/IEC 17799:2005 – Módulo 1.**

MORAES, L. V. S. **A dinâmica da aprendizagem gerencial:** o caso do Hospital Moinhos de Vento. Dissertação de Mestrado, Engenharia de Produção, Centro tecnológico, Universidade Federal de Santa Catarina, 2000.

NAKAMURA, Emílio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. 2ª ed. São Paulo: Futura, 2003. 474 p.

PMF. **Perfil de Florianópolis.** Santa Catarina, nov. 2009. Disponível em: http://www.pmf.sc.gov.br/portal/pmf/cidade/perfildeflorianopolis/demografia.php. Acesso em: 02 nov. 2009.

SILVA FILHO, Antonio Mendes da. A Era da Informação. **Revista Espaço Acadêmico**, Maringá, n. 2, jul., 2001. ISSN: 1519.6186. Disponível em: http://www.espacoacademico.com.br/002/02col_mendes.htm. Acesso em: 15 fev. 2006.

STRAUSS, Anselm L.; CORBIN, Juliet M. **Basics of qualitative research:** Grounded Theory procedures and techniques. CA: SAGE Publications, 1990. 270 p.

UFSC(a). **Universidade Federal de Santa Catarina.** Santa Catarina, out. 2009. Disponível em: http://www.ufsc.br. Acesso em 01 out. 2009.

_____(b), Reitoria da. **Proposta Orçamentária 2009.** Santa Catarina, nov. 2009. Disponível em: http://www.reitoria.ufsc.br/dgo/orcamento%20atual.PDF. Acesso em: 01 nov. 2009.

WIKIPEDIA(a). **Demografia**. Disponível em: http://pt.wikipedia.org/wiki/Demografia. Acesso em 02 nov. 2009.

_____(b). **Lista de instituições de ensino superior no Brasil.** Disponível em: http://pt.wikipedia.org/wiki/Lista_de_universidades_brasileiras. Acesso em: 02 nov. 2009.

_____(c). **Fatores críticos de sucesso.** Disponível em: http://pt.wikipedia.org/wiki/Fatores_cr%C3%ADticos_de_sucesso. Acesso em: 02 nov. 2009.

YIN, Robert K. **Case Study Research:** Design and Methods. 2ª Ed. Thousand Oaks, CA: SAGE Publications, 1994.

GLOSSÁRIO

Access Point - Referido com o acrônimo AP (Ponto de Acesso) é um dispositivo em uma rede sem fio que realiza a interconexão entre todos os dispositivos móveis. Em geral se conecta a uma rede cabeada servindo de ponto de acesso para uma outra rede, como por exemplo a Internet.

Ativo - Qualquer coisa que tenha valor para a organização.

AUP - *Acceptable Use Policy* (Política de Uso Aceitável).

BGP - Acrônimo de *Border Gateway Protocol* é um protocolo de roteamento dinâmico, utilizado para comunicação entre sistemas autônomos (ASs). A função primária de um sistema BGP é trocar informação de acesso à rede, inclusive informação sobre a lista das trajetórias dos ASs, com outros sistemas BGP. Esta informação pode ser usada para construir um gráfico da conectividade dos ASs a partir do qual loops de roteamento podem ser detectados e reforçadas as políticas de decisão com outros ASs.

Cluster - Um *cluster*, ou aglomerado de computadores, é formado por um conjunto de computadores, que utiliza um tipo especial de sistema operacional classificado como sistema distribuído. Muitas vezes é construído a partir de computadores convencionais (*personal computers*), os quais são ligados em rede e comunicam-se através do sistema, trabalhando como se fossem uma única máquina de grande porte. Há diversos tipos de *cluster*. Um tipo famoso é o cluster da classe Beowulf, constituído por diversos nós escravos gerenciados por um só computador.

DMZ – Abreviação de DeMilitarized Zone (zona desmilitarizada). É a área de rede que permanece entre a rede interna de uma organização e uma rede externa, em geral a Internet. Comumente uma DMZ contêm equipamentos apropriados para o acesso à Internet, como servidores para web (http), servidores de transferência de arquivos (FTP), servidores para correio eletrônico (SMTP) e servidores de resolução de nomes (DNS).

DNS - Acrônimo de *Domain Name System* (Sistema de Nomes de Domínios) é um sistema de gerenciamento de nomes hierárquico e distribuído operando segundo duas definições: examinar e atualizar seu banco de dados e resolver nomes de domínios em endereços de rede (IPs).

Ethernet - Tecnologia de interconexão para redes locais, baseada no envio de pacotes, que define cabeamento e sinais elétricos para a camada física, formato de pacotes e protocolos para a camada de controle de acesso ao meio (Media Access Control – MAC) do modelo OSI.

FTP - Acrônimo de *File Transfer Protocol* (Protocolo de Transferência de Arquivos) pode referir-se tanto ao protocolo quanto ao programa que implementa este protocolo e é uma forma bastante rápida e versátil de transferir arquivos, sendo uma das mais usadas na Internet.

Hardware - Parte física do computador que se pode tocar.

Help Desk - Termo em inglês que designa o serviço de apoio a usuários para suporte e resolução de problemas técnicos em informática, telefonia e tecnologias de informação. Este apoio pode ser tanto dentro de uma empresa (profissionais que cuidam da manutenção de equipamentos e instalações dentro da empresa), quanto externamente (prestação de serviços aos usuários).

HTTP - O *Hyper Text Transfer Protocol* (Protocolo de Transferência de Hipertexto) foi criado para que os navegadores e os servidores web pudessem se comunicar de uma forma padronizada.

Hub-and-spoke - Tipo de topologia na qual o host wireless do USB é o “hub” no centro, e cada dispositivo é a extremidade de um ”spoke”. Cada “spoke” é uma conexão ponto-a ponto entre o host e o dispositivo. Desse modo os hosts wireless USB podem suportar até 127 dispositivos.

IEEE 802 - É uma norma que tem como objetivo definir uma padronização para

redes locais e metropolitanas das camadas 1 e 2 (física e enlace) do modelo OSI para padrão de redes. As normas cuidam de diversos tipos de redes, tais como Ethernet, rede sem fio, fibra ótica, dentre outras.

IGRP - Acrônimo de *Interior Gateway Routing Protocol* (Protocolos Interiores de Roteamento) é um protocolo que foi desenvolvido na década de 80 pela Cisco Systems com o objetivo de fornecer um protocolo robusto para distribuir dentro de um Sistema autônomo (COMO).

IMAP - Acrônimo de *Internet Message Access Protocol* é um protocolo de gerenciamento de correio eletrônico superior em recursos ao POP3. A última versão é o IMAP4. O mais interessante é que as mensagens ficam armazenadas no servidor e o internauta pode ter acesso a suas pastas e mensagens em qualquer computador, tanto por webmail como por cliente de correio eletrônico.

Internet - A Internet é a conexão de várias redes e significa a “rede das redes”.

Log - Em computação é o termo utilizado para descrever o processo de registro de eventos relevantes num sistema computacional. Esse registro pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais.

Login - É o procedimento de autenticação na rede, ou em qualquer outro serviço, informando uma identificação de usuário (nome, matrícula, conta de acesso) e senha.

Mídia - Mídia, ou media, no Brasil e em Portugal. Podemos distinguir os tipos de media relativamente à sua origem. Os tipos de media capturados (vídeo, áudio, fotografia) e os tipos de media sintetizados (texto, gráfico, animação). Uma mídia de armazenamento é o suporte no qual pode se registrar a informação digital. Exemplos: fitas magnéticas, disquetes, discos ópticos.

NAT – Acrônimo de *Network Address Translation* (Tradução de Endereço de Rede) também conhecido como *masquerading* é uma técnica que consiste em reescrever os endereços IP de origem de um pacote, que passam por um roteador ou *firewall*, de maneira que um computador de uma rede interna tenha acesso ao exterior (rede pública), sem divulgar o endereço IP real.

Nobreak, no-break - Veja UPS.

Octeto - O byte de 8 bits é, por vezes, também chamado de octeto, nomeadamente no contexto de redes de computadores e telecomunicações.

OSPF - Acrônimo de *Open Shortest Path First* é um protocolo de roteamento para redes que operam com protocolo IP. Baseado no algoritmo Shortest Path First (menor rota primeiro), o OSPF foi criado para substituir o protocolo RIP empregado no final da década de 1980 na então Arpanet (atual Internet) e que apresentava diversos problemas e limitações para operar satisfatoriamente em uma rede de grande porte.

PABX - *Private Automatic Branch Exchange* (Troca automática de ramais privados).

POP, POP3 - Acrônimo de *Post Office Protocol* é um protocolo utilizado no acesso remoto a uma caixa de correio eletrônico e permite que todas as mensagens possam ser transferidas para um computador local.

Protocolo - Conjunto de instruções que padronizam como duas ou mais ferramentas se comunicam. Conjunto de regras padronizado que especifica o formato, a sincronização, a sequencia e a verificação de erros em comunicação de dados.

RIP - Acrônimo de *Routing Information Protocol* é um protocolo de roteamento e um dos mais facilmente confundidos porque uma variedade RIP -como dos protocolos do roteamento proliferados, alguns se usaram do mesmo nome.

ROI - *Return of investiment* (Retorno sobre Investimento).

Roteador - Estrangeirismo do inglês *router* (encaminhador) é um equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores, provendo a comunicação entre computadores distantes entre si.

Roteamento - No contexto das redes de computadores o encaminhamento (ou roteamento) de pacotes (em inglês: *routing*) designa o processo de re-encaminhamento de pacotes, baseado no endereço IP e máscara de rede dos mesmos.

Servidor - Numa rede é o computador que hospeda os arquivos ou recursos que serão acessados pelos demais micros da rede.

Sistema operacional - É um programa ou um conjunto de programas cuja função é servir de interface entre um computador e o usuário. A sigla usual para designar este tipo de programa é SO (em português) ou OS (do inglês *Operating System*).

SMTP - Acrônimo de *Simple Mail Transfer Protocol* éo protocolo padrão para envio de e-mails através da Internet.

SNMP - Acrônimo de *Simple Network Management Protocol* (Protocolo Simples de Gerência de Rede) é um protocolo de gerência típica de redes TCP/IP, da camada de aplicação, que facilita o intercâmbio de informação entre os dispositivos de rede, como placas e comutadores (switches). O SNMP possibilita aos administradores de rede gerenciar o desempenho da rede, encontrar e resolver seus eventuais problemas, e fornecer informações para o planejamento de sua expansão, dentre outras.

Software - É a parte lógica do computador, aquela que não se pode ver nem tocar, mas opera constantemente.

Spanning Tree - Referido com o acrônimo STP é um protocolo para equipamento

de rede que permite resolver problemas de *loop* em redes comutadas cuja topologia introduza anéis nas ligações. O algoritmo de Spanning Tree determina qual é o caminho mais eficiente entre cada segmento separado por bridges ou switches. Caso ocorra um problema nesse caminho, o algoritmo recalculará, entre os existentes, o novo caminho mais eficiente, habilitando-o automaticamente.

Switch - Dispositivo utilizado em redes de computadores para re-encaminhar frames entre diversos nós. Segmenta a rede internamente, sendo que cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisão entre pacotes de segmentos diferentes. Existe modelo gerenciável e não gerenciável.

TCP/IP - Acrônimo de *Transmission Control Protocol / Internet Protocol* (Protocolo de Controle de Transmissão / Protocolo de Internet), é a família de protocolos para a comunicação de dados inter-redes. Hoje é um padrão de fato para inter-redes abertas e seu uso é amplamente difundido no mundo.

Topologia de rede - Descreve como é o *layout* de uma rede de computadores e também como os dispositivos estão conectados a ela.

Trunking - Para manter a conectividade das Vlans em toda a estrutura do switch, as Vlans devem ser configuradas em cada switch. O protocolo VTP (Vlan Trunking Protocol) da Cisco garante um método mais fácil para a manutenção de uma configuração de Vlan consistente em toda a rede comutada.

UPS - Acrônimo de *Uninterruptible Power Supply* (Fonte Ininterrupta de Energia) é o que costumamos chamar de nobreak ou no-break. Existem dois tipos de UPS: os que funcionam no modo on-line e os que funcionam no modo off-line. No modo on-line a bateria é constantemente carregada e o sistema recebe energia a partir da bateria. Neste caso temos a garantia de um fornecimento 100% estável, dispensando um estabilizador externo. No modo off-line o sistema recebe energia da tomada, passando para a bateria apenas em caso de queda. Não é tão seguro quanto o primeiro, mas são mais comuns por serem um pouco mais baratos.

Vírus - Um tipo de software malicioso que tem a habilidade de auto-replicar e infectar partes do sistema operacional ou dos programas de aplicação, com o intuito de causar a perda ou dano dos dados.

VLAN - Acrônimo de *Virtual LAN* (Rede Local Virtual) é uma rede logicamente independente. Várias VLANs podem co-existir em um mesmo comutador (switch), desde que esta funcionalidade exista.

VoIP - Acrônimo de *Voice Over IP* (Voz Sobre IP) é a tecnologia que torna possível estabelecer conversações telefônicas em uma rede IP (incluindo a Internet), tornando a transmissão de voz mais um serviço suportado pela rede de dados.

VPN - Acrônimo de *Virtual Private Network* (Rede Particular Virtual) é uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet). O tráfego de dados é transportado pela rede pública utilizando protocolos padrão, não necessariamente seguro. VPNs seguras usam protocolos de criptografia por tunelamento que fornecem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações requeridas. Quando adequadamente implementados, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

Web - É considerada a rede mundial de computadores que trocam informações através do protocolo HTTP. A Web é o serviço mais usado na Internet e, dependendo do contexto, pode significar o mesmo que Internet.

WWW - Acrônimo de *World Wide Web* (Rede de alcance mundial), também conhecida como Web, é um sistema de documentos em hipermídia que são interligados e executados na Internet.

APÊNDICES

Apêndice I - Plano de Gerenciamento dos Riscos

Nome do Projeto:	Plano de Segurança do EQA - UFSC
Patrocinadores:	Sr. Álvaro Toubes Prata (Reitor da UFSC)
Gerente de Projeto:	Sandro dos Santos
Elaborado por:	Sandro dos Santos Souza
Data Versão:	18/06/2009 - V1.0
Data Elaboração:	05/06/2009

1. Processo de Gerenciamento de Riscos

- Serão considerados os riscos inicialmente identificados pela equipe de projetos
- Novos riscos encontrados no decorrer do projeto serão analisados pela equipe e considerados
- A pesquisa de campo será utilizada como base para identificação dos riscos
- A base da pesquisa e relação dos riscos é baseada nas informações de um membro do grupo.

2. Identificação dos Riscos

A tabela abaixo apresenta os riscos apurados pela equipe no desenvolvimento do projeto.

Riscos considerados	
Riscos internos	Ataques, acesso a conteúdo indevido, concentração de informação, apropriação indevida da informação (espionagem industrial)
Riscos físicos	Ataques, estrutura de cabeamento, uso indevido de recursos
Riscos externos	Falta de energia, desastre natural, mudança da política interna (mudança da chefia)
Riscos técnicos	Uso inadequado dos recursos computacionais, perda de informações (falta de backup)
Riscos legais	Vazamento de informação, furto de informação, utilização de software não homologado, contratos (SLA), pirataria, violação de direitos autorais
Riscos não técnicos	Recursos humanos sem treinamento, cultura

3. Qualificação dos Riscos

a. Avaliação de impacto

Grau de impacto	Peso
Muito grande	5
Grande	4
Moderado	3
Pequeno	2
Muito pequeno	1

b. Descritivo dos impactos

- **Muito Grande:** O impacto é extremamente elevado, sendo necessária interferência direta, imediata e precisa da equipe do projeto, para que os resultados não sejam seriamente comprometidos.
- **Grande:** Impacto de maior relevância, necessitando de um gerenciamento mais preciso, podendo prejudicar os resultados.
- **Moderado:** Impacto considerado relevante, necessitando uma maior atenção em sua análise e resolução, oferecendo risco moderado aos resultados.
- **Pequeno:** O impacto pequeno, em termos de custos ou prazos, fácil solução.
- **Muito Pequeno:** Impacto quase que irrelevante, de fácil solução

c. Avaliação de probabilidade

Referencial	Probabilidade
Grande chance de ocorrer	0.95
Provavelmente ocorrerá	0.75
Igual chance de ocorrer ou não	0.5
Baixa chance de ocorrer	0.25
Pouca chance de ocorrer	0.1

d. Descritivo das probabilidades

- **Grande chance de ocorrer:** a probabilidade de ocorrência é iminente (maior que 80%)
- **Provavelmente ocorrerá:** probabilidade importante de ocorrer (de 60 a 80%)
- **Igual chance de ocorrer ou não:** probabilidade razoável de ocorrer (de 20 a 40%)
- **Pouca chance de ocorrer:** probabilidade quase que imperceptível (menor que 20%)

e. Priorização de Riscos

Baixo Risco	**de 0.1 a 0.75**
Médio Risco	**de 0.95 a 1.9**
Alto Risco	**de 2.0 a 4.75**

f. Matriz de Probabilidade X Impacto

	1.0	**2.0**	**3.0**	**4.0**	**5.0**
0.95	0.95	1.9	2.85	3.8	4.75
0.75	0.75	1.5	2.25	3	3.75
0.5	0.5	1	1.5	2	2.5
0.25	0.25	0.5	0.75	1	1.25
0.1	0.1	0.2	0.3	0.4	0.5

g. Relacionamentos dos Eventos X Probabilidade X Impacto

Seq.	Evento	Probabilidade	Impacto	Matriz
15	Perda de informação	0,95	5	4,75
10	Interrupção do acesso à rede	0,75	5	3,75
1	Ataque de negação de serviço de grande impacto	0,50	5	2,50
31	Vandalismo contra equipamento do EQA	0,25	5	1,25
7	Impossibilidade de acesso ao conhecimento tácito	0,10	5	0,50
12	Falta de energia (blackout)	0,10	5	0,50
13	Desastres naturais	0,10	5	0,50
24	Sinistro ocasionado pelo fogo	0,10	5	0,50
25	Sem registro, documentação dos processos e fluxo da informação, rede, documentação da estrutura	0,95	4	3,80
17	Furto de informação	0,75	4	3,00
22	Ambiente e Cultura da organização	0,75	4	3,00
30	Indisponibilidade de suporte técnico	0,75	4	3,00
8	Apropriação indevida da informação (espionagem industrial)	0,50	4	2,00
26	Senha fraca utilizada em equipamento servidor	0,50	4	2,00
29	Instalação não autorizada de ativos de rede (switch, hub e ponto de acesso wireless)	0,50	4	2,00
2	Ataque de negação de serviço de médio impacto	0,25	4	1,00
16	Vazamento de informação (acesso físico ou lógico)	0,25	4	1,00
32	Rastreabilidade dos desktops do Departamento devido a utilização de IPs válidos (IPs públicos)	0,25	4	1,00
4	Acesso a conteúdo indevido (alto impacto): Pedofilia, Racismo, documentos confidenciais	0,10	4	0,40
5	Acesso a conteúdo indevido (médio impacto): Sexo, pornografia e pedofilia	0,95	3	2,85
11	Uso indevido de recursos	0,95	3	2,85
14	Uso inadequado dos recursos computacionais	0,95	3	2,85
21	Usuários acessando informações e recursos sem o devido treinamento	0,75	3	2,25
28	Ataques a rede através de varreduras no sistema (sniffer)	0,75	3	2,25

Seq.	Evento	Probabilidade	Impacto	Matriz
18	Violação de direitos autorais	0,50	3	1,50
19	Contratos (SLA ou Terceirização)	0,50	3	1,50
20	Pirataria (Obtenção de benefício com software não homologado)	0,50	3	1,50
23	Descontinuidade da política interna devido a mudança da direção em cargos eletivos	0,50	3	1,50
27	Ataques utilizando Engenharia Social	0,50	3	1,50
3	Ataques DoS de baixo impacto: FTP	0,25	3	0,75
9	Ataque físico: Acesso não autorizado a ambientes restritos	0,75	2	1,50
6	Acesso a conteúdo indevido (baixo impacto): outros conteúdos	0,95	1	0,95

4. Quantificação dos Riscos

1 - Ataque de negação de serviço: serviço HTTP	
Tempo do atraso caso ocorra	2 horas
Custo do atraso	R$ 1.000,00
Fatores considerados	Retrabalho; 1 analista, por R$ 60,00/h; 1 técnico, por R$ 25,00/h; Trabalho estimado: de 30 min a 2 horas.
Probabilidade de ocorrência	5%
Valor monetário esperado	R$ 50,00
2 - Ataque de negação de serviço: serviço Webmail	
Tempo do atraso caso ocorra	2 horas
Custo do atraso	R$ 1.000,00
Fatores considerados	Retrabalho; 1 analista, por R$ 60,00/h; 1 técnico, por R$ 25,00/h; Trabalho estimado: de 30 min a 2 horas.
Probabilidade de ocorrência	20%
Valor monetário esperado	R$ 200,00
3 - Ataque de negação de serviço: serviço wireless	
Tempo do atraso caso ocorra	1 hora
Custo do atraso	R$ 250,00
Fatores considerados	Retrabalho; 1 técnico, por R$ 25,00/h; Trabalho estimado: de 30 min a 1 hora.

Probabilidade de ocorrência	25%
Valor monetário esperado	R$ 62,50
4 - Ataque de negação de serviço: serviço de impressão	
Tempo do atraso caso ocorra	2 horas
Custo do atraso	R$ 100,00
Fatores considerados	Retrabalho; 1 técnico, por R$ 25,00/h; Trabalho estimado: de 30 min a 2 horas.
Probabilidade de ocorrência	30%
Valor monetário esperado	R$ 30,00
5 - Ataque de negação de serviço: serviço FTP	
Tempo do atraso caso ocorra	2 horas
Custo do atraso	R$ 1.000,00
Fatores considerados	Retrabalho; 1 técnico, por R$ 25,00/h; Trabalho estimado: de 30 min a 2 horas.
Probabilidade de ocorrência	10%
Valor monetário esperado	R$ 10,00
6 - Acesso a conteúdo indevido: pedofilia, racismo e documentos confidenciais	
Tempo para reverter o dano	3 meses
Custo do risco	R$ 500.000,00
Fatores considerados	3 advogados, por R$ 60.000,00 (custas do processo); marketing, por R$ 100.000,00; treinamento, por R$ 100.000,00; 1 especialista de segurança, R$ 10.000,00/mês; recurso técnico, por R$ 200.000,00.
Probabilidade de ocorrência	30%
Valor monetário esperado	R$ 150.000,00
7 - Acesso a conteúdo indevido: sexo e pornografia	
Tempo para reverter o dano	3 meses
Custo do risco	R$ 100.000,00
Fatores considerados	Advogado, por R$ 10.000,00; marketing; treinamento; 1 especialista em segurança, por R$ 30.000,00; recurso técnico, por R$ 100.000,00.
Probabilidade de ocorrência	50%

Valor monetário esperado	R$ 50.000,00
8 - Acesso a conteúdo indevido: outros conteúdos	
Tempo para reverter o dano	3 meses
Custo do risco	R$ 100.000,00
Fatores considerados	1 advogado, por R$ 20.000,00; 1 especialista em segurança,
Probabilidade de ocorrência	50%
Valor monetário esperado	R$ 50.000,00
9 - Concentração de informação	
Tempo do atraso caso ocorra	5 anos
Custo do atraso	R$ 200.000,00
Fatores considerados	1 especialista em segurança, por R$ 30.000,00; 1 analista, por R$ 15.000,00; recurso técnico, por R$ 50.000,00
Probabilidade de ocorrência	50%
Valor monetário esperado	R$ 100.000,00
10 - Apropriação indevida da informação	
Tempo do atraso caso ocorra	6 meses
Custo do atraso	R$ 250.000,00
Fatores considerados	1 especialista em segurança, por R$ 7.000,00/mês; 1 analista, por R$ 5.000,00/mês; recurso técnico.
Probabilidade de ocorrência	10%
Valor monetário esperado	R$ 25.000,00
11 - Ataque físico	
Tempo do atraso caso ocorra	15 dias
Custo do atraso	R$ 50.000,00
Fatores considerados	1 especialista em segurança, por R$ 7.000,00/mês; 1 analista, por R$ 5.000,00/mês; recurso técnico.
Probabilidade de ocorrência	10%
Valor monetário esperado	R$ 5.000,00
12 - Estrutura de cabeamento em desconformidade com as Normas	
Tempo do atraso caso ocorra	3 dias
Custo do atraso	R$ 20.000,00

Fatores considerados	1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$ 10.000,00
13 - Uso indevido de recursos	
Tempo do atraso caso ocorra	1 dia
Custo do atraso	R$ 5.000,00
Fatores considerados	1 especialista em segurança, por R$ 7.000,00/mês; 1 analista, por R$ 5.000,00/mês; recurso técnico.
Probabilidade de ocorrência	50 %
Valor monetário esperado	R$ 2.500,00
14 - Falta de energia elétrica	
Tempo do atraso caso ocorra	1 hora
Custo do atraso	R$ 100.000,00
Fatores considerados	1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	10%
Valor monetário esperado	R$ 10.000,00
15 - Desastres naturais	
Tempo do atraso caso ocorra	3 dias
Custo do atraso	R$ 250.000,00
Fatores considerados	1 analista, por R$ 5.000,00/mês; 3 técnico de redes R$ 2.000,00/mês cada recurso técnico.
Probabilidade de ocorrência	1 %
Valor monetário esperado	R$ 2.500,00
16 - Uso inadequado dos recursos computacionais	
Tempo do atraso caso ocorra	1 dia
Custo do atraso	R$ 5.000,00
Fatores considerados	1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%

Valor monetário esperado	R$ 2.500,00
17 - Perda da informação, vazamento da informação, furto da informação	
Tempo do atraso caso ocorra	3 meses
Custo do atraso	R$ 500.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$250.000,00
18 - Violação de direitos de copyright	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 300.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$ 150.000,00
19 - Contratos (SLA ou Terceirizados)	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 advogado especialista R$ 5.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$50.000,00
20 - Pirataria (obtenção de benefícios com produtos não homologados)	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 200.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00

	recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$100.000,00
21 - Usuários acessando informações e recursos, sem o devido tratamento	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$50.000,00
22 - Ambiente e cultura da organização	
Tempo do atraso caso ocorra	12 meses
Custo do atraso	R$ 500.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$250.000,00
23 - Descontinuidade de política interna devido a mudança da direção em cargos eletivos	
Tempo do atraso caso ocorra	24 meses
Custo do atraso	R$ 500.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$250.000,00
24 - Sinistro ocasionado pelo fogo	
Tempo do atraso caso ocorra	12 meses
Custo do atraso	R$ 1.000.000,00

Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	10%
Valor monetário esperado	R$100.000,00
25 - Sem registro, documentação dos processos e fluxo da informação, rede, documentação da estrutura	
Tempo do atraso caso ocorra	6 meses
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 Recurso técnico.
Probabilidade de ocorrência	75%
Valor monetário esperado	R$ 75.000,00
26 - Senhas fracas utilizadas nos servidores e desktops	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	80%
Valor monetário esperado	R$80.000,00
27 - Ataques utilizando Engenharia Social	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 250.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$ 125.000,00

28 - Ataques a rede através de varreduras ao sistema (sniffer)	
Tempo do atraso caso ocorra	1 semana
Custo do atraso	R$ 50.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$25.000,00
29 - Instalação não autorizada de ativo de rede (switch, hub, ponto de acesso wireless)	
Tempo do atraso caso ocorra	1 semana
Custo do atraso	R$ 20.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	50%
Valor monetário esperado	R$10.000,00
30 - Alta rotatividade da equipe de TI	
Tempo do atraso caso ocorra	12 meses
Custo do atraso	R$ 300.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês recurso técnico.
Probabilidade de ocorrência	70%
Valor monetário esperado	R$210.000,00
31 – Vandalismo (desligamento ou dano a equipamento)	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	10%

Valor monetário esperado	R$ 10.000,00
32 – Rastreabilidade na rede dos desktops do Departamento devido a utilização de IP´s válidos (IPs públicos)	
Tempo do atraso caso ocorra	1 mês
Custo do atraso	R$ 100.000,00
Fatores considerados	1 especialista e segurança da informação R$ 7.000,00/mês 1 analista, por R$ 5.000,00/mês; 1 técnico de redes R$ 2.000,00 recurso técnico.
Probabilidade de ocorrência	90%
Valor monetário esperado	R$90.000,00

5. Respostas aos Riscos

Item	Risco
1 – 5	**Ataque de negação de serviço (HTTP, Webmail, wireless, impressão e FTP)**
Classificação	Alto
Etapa	Inicial
Gatilho	Análise do log de monitoramento, gerado quando ocorre a tentativa de negação do serviço.
Resposta	Medidas preventivas para evitar a efetivação do risco; Reconfigurar o firewall; Acionar a equipe de resposta a incidentes.
Descrição	Manter os sistemas atualizados e monitorados.
Custo	R$ 80.000,00
Responsável	Administrador da rede.
Item	Risco
6 – 8	**Acesso a conteúdo indevido (pedofilia, racismo, documentos confidenciais, sexo, pornografia e outros conteúdos)**
Classificação	Alto
Etapa	Inicial
Gatilho	Análise do log de monitoramento.
Resposta	Medidas preventivas para evitar a efetivação do risco.
Descrição	Reconfigurar o proxy; Fazer campanha de conscientização entre os usuários (AUP).

Custo	R$ 2.500,00
Responsável	Administrador da rede.
Item	Risco
9	**Concentração de informação**
Classificação	Alto
Etapa	Inicial
Gatilho	Levantamento de unicidade de repositórios de informação (apenas um professor em determinada linha de pesquisa).
Resposta	Definir políticas de redundância da informação (backup de mídias magnéticas; pluralidade de professores por linha de pesquisa; diversificação dos meios de transporte para professores do mesmo Departamento); Revisar as disciplinas ministradas pelos professores.
Descrição	Distribuir e documentar as informações relevantes
Custo	R$ 25.000,00
Responsável	Administrador da rede e Chefe do Departamento
Item	Risco
10	**Apropriação indevida da informação**
Classificação	Alto
Etapa	Inicial
Gatilho	Identificação de uma informação restrita ou confidencial disponível a terceiros; Detecção através de análise de logs de acesso.
Resposta	Aplicação da legislação legal; Desenvolver uma política de conscientização para os usuários; Rever as regras de controle de acesso; Rever política de classificação da informação. Cuidar com o fluxo de informação na organização (criptografia, envelope lacrado, livro de registrado de entrada e saída de documentos etc..)
Descrição	Resguardar as informações de modo a protegê-las de acessos indesejados
Custo	R$ 200.000,00
Responsável	Equipe de segurança da informação
Item	Risco
11	**Ataque físico**
Classificação	Alto
Etapa	Inicial

Gatilho	Identificação de invasão a ambiente de acesso restrito.
Resposta	Sinalização “Área de acesso restrito”; Sistema de monitoramento com câmeras; Sistema de identificação de acesso através do uso de fechadura eletrônica; Treinamento dos funcionários responsáveis pelo controle do acesso físico.
Descrição	Manter as áreas sinalizadas e monitoradas buscando controle dos acessos.
Custo	R$ 50.000,00
Responsável	Segurança patrimonial.
Item	Risco
12	**Estrutura de cabeamento em desconformidade com as Normas**
Classificação	Alto
Etapa	Intermediária
Gatilho	Ocorrência de interrupção de aceso à rede; Diminuição do índice de disponibilidade da rede; Throuput reduzido.
Resposta	Revisão da rede para correção das irregularidades.
Descrição	Certificação da rede de cabeamento.
Custo	R$ 150.000,00
Responsável	Equipe de infraestrutura de redes.
Item	Risco
13	**Uso indevido de recursos**
Classificação	Médio
Etapa	Intermediária
Gatilho	Logs de registro; Serviços detectados no(s) servidor(es) incompatível com atividade do usuário; Uso excessivo de banda para download não autorizado.
Resposta	Campanha de conscientização dos usuários; Fiscalização dos recursos pela equipe de administração da rede.
Descrição	Monitorar os acesso a recursos computacionais buscando minimizar custos e aumentar a segurança.
Custo	R$ 3.000,00
Responsável	Administrador da rede
Item	Risco

14	**Falta de energia elétrica**
Classificação	Alto
Etapa	Inicial
Gatilho	Interrupção do serviço pela concessionária
Resposta	Utilização de no-break e gerador de energia.
Descrição	Manter o no-break e o gerador de energia em condições para entrarem em funcionamento a qualquer momento; Definir áreas prioritárias para recebimento dos no-breaks; Combinar com as áreas um esquema de revezamento para utilização do gerador.
Custo	R$ 250.000,00
Responsável	Equipe de logística
Item	Risco
15	**Desastres Naturais**
Classificação	Baixa
Etapa	Intermediaria
Gatilho	Alertas gerados pelas organizações responsáveis por desastres, como por exemplo a Defesa Civil local, Brigada de incêndio, CIPA.
Resposta	Ações de respostas aos alertas emitidos pelos órgãos competentes, por exemplo, evacuação do recinto, desligamento da energia elétrica, retirada física dos servidores dos locais de trabalho, acionamento da brigada de incêndio.
Descrição	Estar sempre em estado de alerta, treinamento de equipe para resposta ao sinistro como objetivo de redução do dano.
Custo	R$ 350.000,00
Responsável	Divisão de Segurança e Saúde do Trabalhador – DSST e o Departamento de Segurança Patrimonial do Campus UFSC – DST.
Item	Risco
16	**Uso inadequado dos recursos computacionais**
Classificação	Alto
Etapa	Intermediária
Gatilho	Serviço interrompido ou ineficiente.
Resposta	Definição de um padrão aceitável de utilização.
Descrição	Definição de um AUP (política de uso aceitável dos recursos computacionais); treinamento dos usuários e monitoramento do uso dos recursos.
Custo	R$ 50.000,00

Responsável	Chefe do Departamento e Administrador da rede.
Item	Risco
17	**Perda da informação, vazamento da informação, furto da informação.**
Classificação	Alto
Etapa	Inicial
Gatilho	Reclamações dos usuários, retrabalho, constatação de apropriação de informações a pessoas não autorizadas.
Resposta	**ABNT NBR ISO/IEC 17799**
Descrição	Criar uma **política de backup;** definir um protocolo para o tratamento da informação com classificação: **Restrito – Uso Interno – Confidencial** e aplicação da **ABNT NBR ISO/IEC 17799;** restringir o acesso à informação; definir políticas de segurança, como por exemplo, definir áreas restritas ao acesso de pessoas; desabilitar portas USB de CPUs; possuir na organização máquinas fragmentadoras de papel. Cuidar do fluxo de informação na organização (criptografia, envelope lacrado, livro de registro de entrada e saída de documentos em trânsito etc..); definir responsável pelo tratamento das informações consideradas criticas pela organização.
Custo	R$ 150.000,00
Responsável	Donos, manipuladores das informações
Item	Risco
18	**Violação dos direitos de copyright**
Classificação	Alto
Etapa	Inicial
Gatilho	Verificação de utilização de software não homologado, grande número de cópias de livros, artigos, normas em empresas de fotocopiadoras no Campus.
Resposta	Educação e um convênio, com estas empresas detentoras dos direitos autorais, com a intenção de facilitar o acesso aos seus produtos com redução do preço de aquisição.
Descrição	Uma campanha de educação com enfoque a respeito aos direitos autorais.
Custo	R$ 100.000,00
Responsável	A direção da UFSC
Item	Risco
19	**Contratos (SLA ou Terceirizados)**
Classificação	Alto

Etapa	Final
Gatilho	Evasão de informações, espionagem industrial
Resposta	SLA, Contrato
Descrição	Elaboração de um contrato que defini claramente as responsabilidades da Empresa terceirizado com o trato das informações do Departamento EQA.
Custo	R$ 15.000,00
Responsável	Chefe do EQA
Item	Risco
20	**Pirataria (obtenção de benefícios com produtos não homologados)**
Classificação	Alto
Etapa	Inicial
Gatilho	Detecção de revenda de software e venda de xérox de livros em bancas
Resposta	Campanha para conscientizar os usuários do problema de comercialização e aquisição produtos pirateados
Descrição	Campanha de conscientização e aumento da fiscalização com o acionamento da Policia Federal
Custo	R$ 50.000,00
Responsável	Administração Central da UFSC
Item	Risco
21	**Usuários acessando informações e recursos, sem o devido treinamento**
Classificação	Alto
Etapa	Intermediaria
Gatilho	Perda de informações, inviabilizarão de recursos computacionais, fragilização da segurança das informações
Resposta	Treinamento, definição clara das responsabilidades do usuário
Descrição	Realização de treinamento para os usuários, definição de uma Política de Uso Aceitável (AUP) para os recursos do Departamento.
Custo	R$ 50.000,00
Responsável	Direção do EQA
Item	Risco
22	**Ambiente e cultura da organização**
Classificação	Alto

Etapa	Final
Gatilho	Descaso pelos usuários com as normas da organização
Resposta	Campanha de conscientização, rigidez nos processos administrativos, implantar uma política de valorização da ética profissional na organização
Descrição	Campanha de conscientização, ética profissional, rigidez nos processos administrativos de funcionários na organização, minimização do corporativismo existente na organização, eliminar a politização dos cargos da organização (meritrocacia)
Custo	R$ 50.000,00
Responsável	Direção do Departamento
Item	Risco
23	**Descontinuidade de política interna da organização devido a mudança da direção em cargos eletivos**
Classificação	Alto
Etapa	Final
Gatilho	Descontinuidade de políticas
Resposta	Definir diretrizes mínimas de uma política na organização
Descrição	Definir diretrizes mínimas de uma política na organização como conhecimento claro pelos usuários da missão, visão, negócio. Diretrizes bem definidas e claras com um planejamento estratégico a curto,médio e longo prazo.
Custo	R$ 50.000,00
Responsável	Direção do EQA
Item	Risco
24	**Sinistro ocasionado pelo fogo**
Classificação	Médio
Etapa	Inicial
Gatilho	Fumaça
Resposta	Definir responsável para desligar equipamentos e relatórios técnicos de acompanhamento das instalações elétricas
Descrição	Definir responsável para desligar os equipamentos principalmente os destiladores em laboratórios e cafeteiras elétricas nas repartições. Instalação de novos equipamentos elétricos somente com aval de um profissional da área elétrica (sobrecarga). Planejamento para instalação de novos equipamentos.
Custo	R$ 5.000,00
Responsável	Supervisores dos Laboratórios
Item	Risco

25	**Sem registro, documentação dos processos e fluxo da informação, rede, documentação da estrutura**
Classificação	Baixo
Etapa	Inicial
Gatilho	Constatação em determinadas situações da necessidade ter acesso a registro, documentação, planta para poder resgatar uma determinada informação.
Resposta	Documentar, registrar, mapear as informações
Descrição	Documentar, registrar, mapear as informações
Custo	R$ 5.000,00
Responsável	Direção do EQA
Item	Risco
26	**Senhas fracas utilizados nos servidores e desktops**
Classificação	Alto
Etapa	Inicial
Gatilho	Constatação de acesso de pessoas não autorizadas a determinados sistemas
Resposta	Definir e aplicar normas para elaboração de senhas para repositórios de informação
Descrição	Aplicar um sistema de gerenciamento de senha conforme a ABNT ISO/IEC 17799
Custo	R$ 1.000,00
Responsável	Direção do EQA e administrador de rede
Item	Risco
27	**Ataques utilizando Engenharia Social**
Classificação	Alto
Etapa	Intermediária
Gatilho	Constatação de acesso de pessoas não autorizadas a determinados sistemas, log´s de registro de invasão.
Resposta	Treinamento aos usuários e monitores no sistema para detectar invasões
Descrição	Treinamento aos usuários com relação a abordagem de algum agente utilizando engenharia social para ter acesso a alguma informação da organização, colocação de IDS no sistema
Custo	R$ 1.000,00
Responsável	Direção do EQA e administrador de rede
Item	Risco

28	**Ataques a rede através de varreduras ao sistema (sniffer)**
Classificação	Alto
Etapa	Inicial
Gatilho	Log´s de sistema de detecção de intrusos ao sistema
Resposta	Monitorar e avaliar os log´s de ocorrência destes eventos
Descrição	Monitorar e avaliar os log´s de ocorrência destes eventos, reengenharia da rede no intuito de sanar possíveis vulnerabilidades
Custo	R$ 1.000,00
Responsável	Direção do EQA e administrador de rede
Item	Risco
29	**Instalação não autorizada de ativo de rede (switch, hub, ponto de acesso wireless)**
Classificação	Alto
Etapa	Intermediária
Gatilho	Constatação de um novo ativo de rede sem o conhecimento da administrador da rede
Resposta	Equipamento novo somente com autorização do administrador de rede
Descrição	Definir uma política onde somente adquiri e instala equipamentos com autorização do administrador com configurações definidas pelo administrador
Custo	R$ 1.000,00
Responsável	Direção do EQA e administrador de rede
Item	Risco
30	**Alta rotatividade da equipe de TI**
Classificação	Alto
Etapa	Intermediária
Gatilho	Constatação de alta rotação da equipe de TI
Resposta	Promover melhorias no ambiente de trabalho bem como valorização salarial.
Descrição	Implantar uma política salarial mais agressiva bem como melhoria no ambiente de trabalho para possibilitar a permanência destes profissionais na organização e motivação. Implantar um política de gestão de pessoal.
Custo	R$ 40.000,00
Responsável	Direção do CTC e direção do EQA
Item	Risco

31	**Vandalismo (desligamento ou dano a equipamento)**
Classificação	Baixo
Etapa	Inicial
Gatilho	Constatação da inoperância de algum serviço
Resposta	Restrição de acesso e monitoramento
Descrição	Restrição de acesso e monitoramento
Custo	R$ 50.000,00
Responsável	Departamento de Segurança Patrimonial
32	**Rastreabilidade na rede dos desktops do Departamento devido a utilização de IP´s válidos (IP´s públicos)**
Classificação	Alto
Etapa	Intermediaria
Gatilho	Constatação de invasão de algum desktop por agentes externos a rede interna. Log´s de sistema de monitoramento
Resposta	Firewall, IDS, IPS
Descrição	Configuração de Firewall, criação de zonas desmilitarizadas, implantação de sistemas de detecção de invasão e sistemas de prevenção de invasão
Custo	R$ 250.000,00
Responsável	Administrador da Rede

6. Reservas de Contingência

São reservas destinadas exclusivamente ao processo de gerenciamento de risco, identificados no planejamento como aceitáveis, e para os riscos não identificados de modo preliminar no projeto

As reservas serão usadas de acordo com as solicitações de mudança e dentro da autonomia do gerente de projeto e também do aval do patrocinador. As ações de contorno ou respostas aos riscos devem utilizar exclusivamente as reservas de contingência do projeto.

As reservas de contingência totalizaram 2.232.942,50 e o gerente de projeto tem as seguintes autonomias quanto à utilização das reservas:

Reservas de Contingência	
Gerente de projeto isoladamente	Até 25% do valor da contingência
Gerente de projeto com aval do patrocinador	Até 50% do valor da contingência
Somente o patrocinador	Acima de 50% e até o limite das reservas

7. Frequência de atualização do Plano de Gerenciamento de Riscos

O plano de Gerenciamento de Riscos será reavaliado trimestralmente nas reuniões realizadas com a equipe de projeto, ou em convocação extraordinária em casos de epidemia de novos riscos.

8. Alocação financeira para o gerenciamento de riscos

Será alocado o valor de R$ 5.803.350,00, para a gestão dos riscos sendo: R$ 2.232.942,50 (reserva de contingência) + 15 % do valor contingenciado R$ 334.941,38 (Riscos não identificados)

9. Responsáveis pela administração do plano

Membros da equipe da especialização em Gestão da Segurança da Informação: Jorge Antônio Coelho de Sousa, Roberto Rivelino Dias, Rossano Cancelier e Sandro do Santos Souza.

10. Registro de Alterações

Registro de Alterações			
Data	Modificado por	Descrição da mudança	Aprovado por
15/06/09	Sandro dos Santos Souza	Ajuste de custos	Sr. Álvaro Toubes Prata - Reitor
18/06/09	Jorge A. Coelho	Identificação de um novo risco (nº 23)	Coordenador do EQA – Prof. Dr. Agenor Furigo Jr.

11. Aprovado por:

_____ _____

Sr. Sandro dos Santos - Ger. do Projeto Sr. Álvaro Toubes Prata - Sponsor

Apêndice II - Proposta de Política de Segurança.

Política UFSC-EQA-100709

Submetido por:	Grupo JRRS	
Aprovado por:	Gestores de Segurança da Informação da UFSC	
Áreas/Unidades:	Esta política é aplicável ao EQA	
Escopo da Política:	Corporativo	
Número da Política:	UFSC-EQA-001/09	
Data de efetivação:	11/07/2009	**Versão:** 2.2

Conteúdo da Política

JUSTIFICATIVA:

Uma política de segurança é um instrumento para proteger a organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais:

- CONFIABILIDADE;
- INTEGRIDADE;
- DISPONIBILIDADE.

Desta forma a política de segurança atribui direitos e responsabilidades a usuários de estações computacionais do EQA bem como todo acesso a rede/EQA.

ASPECTOS PRELIMINARES:

A política de segurança deve cobrir os seguintes aspectos:

- abrangência e escopo de atuação da política;
- definições fundamentais;
- normas e regulamentos aos quais a política está subordinada;
- quem tem autoridade para sancionar, implementar e fiscalizar o cumprimento da política;
- meios de distribuição da política;
- como e com que freqüência a política é revisada;
- definição de uma política de senhas;
- direitos e responsabilidades dos usuários;
- direitos e responsabilidades da administração da rede;
- ações previstas em caso de violação da política.

Escopo e aplicabilidade

Esta política é endereçada ao EQA, seus departamentos, incluindo alunos e funcionários em todos os níveis e formas de contratação.

Nível de aplicabilidade e aceitação

Todas as pessoas as quais esta política for endereçada devem aceitá-la e empregá-la em sua totalidade (100% de aderência).

Circunstâncias Especiais e Exceções

Quando não se puder atender a aplicabilidade e aceitação desta, deverá ser informado ao comitê de segurança por escrito o motivo de não aceitação da mesma para que se possa determinar o correto nível de exceção. Gestores e diretores não estão autorizados a modificar ou criar exceções a esta política.

Definições, acrônimos, termos e palavras chave

Termo	**Definição**
SI	Segurança da Informação
ASD	A Ser Definido
HTTP	Hypertext Transfer Protocol
FTP	File Transfer Protocol
SSL	Secure Sockets Layer
WTLS	Wireless Transport Layer Security
SGBD	Sistema de Gerenciamento de Banco de Dados
Cluster	Aglomerado de computadores
TLS	Transport Layer Security
PGP	*Pretty Good Privacy* (privacidade bastante boa)
RFID	Radio-Frequency Identification (Identificação por Rádio Frequência)
DMZ	DeMilitarized Zone (zona desmilitarizada)
IDS	Intrusion Detection System (sistema de detecção de intrusão)
IPS	Intrusion Prevention System (sistema de prevenção de intruso)
VLAN	Virtual Local Area Network (rede local virtual)

Papéis e responsabilidades

Os papéis e responsabilidades no desenvolvimento desta política incluem:

Papel	Descrição	Detalhes
Patrocinador	Stack holder, ou responsável financeiro	UFSC
Proponente	Órgão solicitante da política	Departamento técnico do EQA
Desenvolvedor	Grupo desenvolvedor da política	Grupo JRRS
Revisor	Responsável pela revisão da política	Departamento técnico do EQA
Aprovador	Responsável pela aprovação da política	Departamento técnico do EQA
Implementador	Responsável pela implementação da política	Departamento técnico do EQA

Os papéis e responsabilidades no desenvolvimento, implementação e supervisão desta política incluem:

Papel	Descrição	Detalhes
Gestão de Negócios	ASD	ASD
Gestão Técnica	Define, implanta, controla e ajusta políticas de segurança	Núcleo de Desenvolvimento e Assessoramento Técnico (NDA)
Segurança de dados	Responsável pela guarda e processamento dos dados da UFSC	Núcleo de Processamento de Dados (NPD)
Gerencia de risco	ASD	ASD
Engenheiro de redes	Responsável pela infraestrutura das redes da UFSC	Núcleo de Processamento de Dados (NPD)

Política de Uso Aceitável

A administração dos recursos computacionais e recursos de rede do EQA, **não autoriza** o uso de sua rede de computadores e estações de trabalho para os seguintes fins:

• Transmitir ou divulgar ameaças, pornografia infantil, material racista, discriminatório ou qualquer outro que viole a legislação em vigor no EQA, na UFSC e do Brasil;

• Propagar vírus de computador ou qualquer programa de computador que possa causar danos permanentes ou temporários em equipamentos de terceiros;

• Transmitir tipos ou quantidades de dados que possam causar falhas em serviços ou equipamentos na rede do EQA ou de terceiros;

• Utilizar computadores ou a rede de computadores do EQA para efetuar levantamento de informações não autorizado (SCAN) na rede de computadores do EQA ou de terceiros;

• Uso da rede de computadores do EQA para o trânsito de mensagens de e-mail com cabeçalhos inválidos ou alterados, de forma a dificultar ou impedir a identificação da sua origem, ou mensagens enviadas através de servidores de e-mail de terceiros, sem a autorização dos respectivos responsáveis (relaying);

• Usar a rede para tentar e/ou realizar acesso não autorizado a dispositivos de comunicação, informação ou computação;

• Utilização dos computadores e redes de computadores do EQA para a coleta de endereços de e-mail dos seus clientes.

• Forjar endereços Internet de máquinas, de rede ou de correio eletrônico, na tentativa de responsabilizar terceiros ou ocultar a identidade ou autoria;

• Destruir ou corromper dados e informações de terceiros;

• Violar a privacidade de terceiros;

• Distribuir via correio eletrônico, grupos de discussão, fóruns e formas similares de comunicação mensagens não solicitadas do tipo 'corrente' e mensagens em massa, comerciais ou não (ver “Política AntiSPAM”);

• Enviar grande quantidade de mensagens idênticas ao mesmo destinatário por correio eletrônico - DoS (mail bombing);

• Transmitir, distribuir ou armazenar materiais protegidos por direito autoral ou quaisquer outros direitos de propriedade intelectual;

• A utilização de recurso computacional e da rede EQA sem o mínimo de conhecimento de uso e manutenção, em níveis aceitável, dos aplicativos, antivírus e ferramentas de manutenção do sistema operacional e atualização do sistema operacional (service pack).

• Navegar sites não recomendados, e o uso de salas de bate-papo (ICQ,IRC, MENSSANGER etc...) que possibilitam a contaminação por WORM e VIRUS a estação de trabalho comprometendo todo a rede EQA;

Obs: O acesso a estes sites fica autorizado fora do horário comercial (18:00 às 7:30) sendo que os usuários que utilizarem estas ferramentas, durante este período, ficam responsáveis por seu uso nas respectivas CPU´s.

• A utilização, devido a sua alta vulnerabilidade, os sistemas operacionais Windows 95, 98 e Millenium para acesso a rede EQ.

• O ingresso de uma nova máquina (nó) ou qualquer outro dispositivo bem como a segmentação da rede EQA sem prévia autorização da administração da rede, inclusive implantação de wlans (wireles lan´s).

• Disponibilizar estações de trabalho e acesso a rede a terceiros sem prévia autorização da administração da rede do EQA.

• Ouvir qualquer tipo de radio on line, filmes via rede (inclusive fazer download´s), jogos de entretenimento em rede, utilizar kazaa ou outro programa de busca de música e multimídia e/ou qualquer outro aplicativo que sature a banda de rede do EQA.

• Quaisquer outros usos que violem a legislação vigente na UFSC e no Brasil.

Regras e ações

A política de uso aceitável tem sua abrangência a instalações computacionais do Departamento/EQA e deverão ser respeitadas pelos seus respectivos usuários;

A fiscalização caberá a administração da rede do EQA;

- A violação destas normas poderá resultar em suspensão temporária ou cancelamento dos serviços prestados, além das demais medidas necessárias, incluindo, mas não se limitando à remoção de dados, desativação de servidores e implementação de filtros. Todos os recursos deverão ser apreciados por uma comissão constituída de: 01 (um) representante do corpo docente, 01 (um) representante do corpo discente e 01 (um) representante do corpo técnico-administrativo eleita pelo chefe do departamento EQA;

- Obedecendo as práticas definidas para a Internet, será mantido o endereço do suporte (suporte@enq.ufsc.br) para servir de canal de reclamação de práticas abusivas vindas da rede de computadores da rede EQA. As pessoas que se sentirem prejudicadas por pacotes de dados vindos de nossa rede devem denunciar a prática enviando um e-mail para esse endereço com informações detalhadas, inclusive registros de computadores (logs), sobre a prática abusiva e como um canal de solicitação de serviços de suporte;

- A administração da rede EQA disponibiliza para os usuários: o programa de antivírus atualizado, treinamento para o uso deste antivírus;
- A UFSC disponibiliza treinamento para uso de aplicativos utilizados no computador através dos projetos OFICINAS e similares;
- O Núcleo de Processamento de Dados da UFSC (NPD) dá suporte ao usuário da rede EQA disponibilizando alguns serviços como por exemplo a remoção de vírus;
- É de responsabilidade do usuário a instalação e manutenção de aplicativos em sua estação de trabalho;
- Todo usuário deve adotar a política de realizar backup (cópia de segurança) de seu material, a administração do EQA não se responsabiliza por possíveis perdas;

Controle de acesso às informações

Após a classificação das informações deve-se definir um sistema que disponibilize a informação conforme o perfil do usuário que desejar acessar o sistema. Isto se consegue através de um sistema de domínio classificando um grupo de usuários, onde cada usuário que acessar o sistema através login/senha ou cartão ou token etc. Possuir acesso somente as informações pré- definidas para o seu perfil.

Acesso Full somente para o Chefe e Sub-Chefe, Coordenadores dos cursos de pós-graduação e dos projetos de ensino, pesquisa e extensão aos demais usuários limitar o acesso somente para as atividades fins.

Local de armazenamento

O Departamento apresenta os seus repositórios de informações dispersos na organização e sem nenhum critério de armazenamento, sem um sistema de redundância, controle de acesso etc..

Recomenda-se que a organização possua um centro de armazenamento das informações para facilitar o controle e acesso. Deve possuir um sistema de armazenamento profissional obtido através de storages ou outra solução similar, bem como a definição do local no ambiente organizacional que seja possível restringir o acesso e que seja seguro contra ataques e a riscos de enchente, fogo, engenharia social, etc.

Solução proposta

A solução para este cenário é ampla e deve ser aplicada nos seguintes pontos:

- A Política de Segurança deve ser revisada/implementada no sentido de impedir o armazenamento de informação sensível nos desktops, smartphones e notebooks, e sim diretamente no servidor de arquivos e de SGBD. Neste último será utilizada criptografia nativa (ex:PGP), para cifragem dos dados. Toda informação será classificada e sua propriedade

definida.

- A Política de Segurança deverá conter também formas de responsabilização dos usuários, inclusive os terceirizados, e definir a quem caberá a guarda e custódia da informação classificada como privada e confidencial.
- Deve prever a periodicidade de revisão do plano de segurança, os critérios para a segurança física da informação e a capacitação dos responsáveis pela sua guarda, visando principalmente evitar ataque de Engenharia Social;
- Para garantir a autenticidade, cada usuário será validado através de uma chave privada, armazenada num token de uso pessoal. Esta chave será utilizada para acesso aos dados do servidor de arquivos e ao SGBD. Desta forma o sistema tentará garantir a confidencialidade das informações apenas para as pessoas autorizadas;
- Nas estações e notebooks dos pesquisadores, os dados deverão ser armazenados utilizando criptografia. A chave privada será armazenada em token ou smart card e, por medida de segurança, uma cópia desta chave será armazenada no EQA. Desta forma, caso o desktop ou o notebook sejam furtados e as suas informações não serão roubadas;
- Para garantir que as informações não serão interceptadas por pessoas não autorizadas, todo o tráfego da rede cabeada, deverá ser criptografado utilizando o protocolo TLS/SSL e o tráfego da rede wireless deverá ser criptografado utilizando o protocolo WTLS;
- Para os sistemas telefônicos implementar o protocolo secvoice para evitar escutas telefônicas (grampos);
- O acesso físico aos ambientes de pesquisa e desenvolvimento acadêmico será controlado, utilizando-se biometria, através de SC RFID, smart card ou token;
- Os servidores de banco de dados e de aplicação deverão ter criptografia na camada de aplicação. Ambos não serão visíveis pela internet e somente serão acessados de forma indireta pelos servidores localizados na DMZ. O acesso remoto será através do protocolo SSL. Os servidores de FTP e HTTP, que não contenham dados sensíveis serão deslocados para a DMZ.
- Disponibilizar o storage numa zona militarizada (firewall, IDS, IPS, Vlan securty, etc..) juntamente com os outros servidores críticos.
- Utilizar criptografia assimétrica para o sistema de e-mail do departamento.

Política dos dispositivos móveis

Os dispositivos móveis devem ser autenticados e ter suas informações criptografadas, através da utilização de token, incluindo o acesso a VPN’s. O equipamento escolhido é o modelo iKey 2032, fornecido pela empresa SafeNet e o aplicativo homologado para iteração é o MS Crypto. A não utilização desta tecnologia, constatada através de auditoria, acarretará nas seguintes punições:

- Na primeira ocorrência: advertência escrita e registro na ficha funcional;
- Na segunda ocorrência: suspensão funcional por 30 dias;
- Na terceira ocorrência: cancelamento do direito de utilização do dispositivo móvel do Departamento;
- Só podem acessar a rede equipamentos da instituição;

Documentação de apoio

Abaixo uma relação de documentos para apoio:

Documento	Origem	Aplicabilidade
ISO 27001	International Organization for Standardization e International Electrotechnical Commision.	Padrão para sistema de gerência da segurança da informação
ISO 17799	International Organization for Standardization e International Electrotechnical Commision.	Conjunto, de recomendações para práticas na gestão de Segurança da Informação
NS110709_v1.0	Equipe JRRS	Define acessos seguros às informações através da utilização de protocolos seguros.

Sanções

As sanções adotadas nesta política são suportadas pela norma interna UFSC-NI-001.

Para maiores detalhes consulte a norma disponível na Intranet corporativa, na seção normas de segurança e sanções.

Histórico de Alterações

Modificado por

Versão	Data	Nome	Função
1.0	10-07-2009	Roberto Rivelino Dias	Coordenação de Segurança da Informação

Controle de Aprovações

Aprovado por

Versão	Data	Nome	Função
1.0	10-07-2009	Rossano Cancelier	CEO

Controle de Revisões

Versão	Nome	Data	Descrição
1.0	Jorge Antônio Coelho de Sousa	10-07-2009	Criação da política

Referências
ISO 27001, ISO 17799

Recursos
N/A

Equipe:
Jorge Antônio Coelho de Sousa
Roberto Rivelino Dias
Rossano Cancelier
Sandro dos Santos Souza

Apêndice III - Plano de contingência do EQA

1. Objetivo

O objetivo deste Plano de Contingência visa assegurar o processo de desenvolvimento contínuo das pesquisas do Departamento de Engenharia Química e Engenharia de Alimentos (EQA) em caso de incidentes, envolvendo falhas de hardware e/ou de software, destruição ou perda de documentos, devido a desastres naturais ou por falha humana, dentre outros, que possam provocar indisponibilidade ou interrupção desta atividade.

Este Plano tem como escopo precípuo a salvaguarda das informações, desenvolvidas e armazenadas nos laboratórios do EQA, inerentes aos projetos de pesquisa.

2. Organização

A organização deste Plano de Contingência é composta por diversos grupos, com funções e características distintas.

Estes grupos serão responsáveis pelas diversas fases e etapas de implantação e ativação do Plano de Contingência.

a) Comitê de Segurança

- Grupo responsável por exercer a coordenação geral do Plano de Contingência;
- Garantir que a restauração das atividades de pesquisa ocorra dentro do prazo estipulado no Plano de Contingência conforme a criticidade de cada projeto;
- Este grupo é composto por membros das seguintes áreas:
    - Pesquisa;
    - Informática;
    - Auditoria;
    - Segurança da Informação.

b) Área de Pesquisa

- Grupo responsável pela coordenação das atividades do Plano de Contingência relacionadas com a área de pesquisa;
- Este grupo é composto por representantes das pesquisas desenvolvidas no EQA:
    - Coordenadores dos CPGENQ, CPGEA;
    - Coordenadores de pesquisa.

c) Apoio Administrativo

- Grupo responsável pela coordenação das atividades administrativas, necessárias para a execução do Plano de Contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NDA (Núcleo de Desenvolvimento e Assessoramento técnico) - TI;
    - Coordenadores dos cursos:
        - CPGENQ;
        - CPGEA;
    - Coordenador dos cursos de Pesquisa.

d) Aplicativos
- Grupo responsável pelo desenvolvimento das aplicações necessárias à execução do Plano de Contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NPD (Núcleo de Processamento de Dados) – TI;
    - NDA – TI:
        - Supervisor do NDA;
    - Coordenadores de pesquisa.

e) Hardware
- Grupo responsável pela coordenação do hardware necessário ao Plano de Contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NDA – TI;
    - NPD – TI:
        - Técnicos e Supervisor do NPD.

f) Software
- Grupo responsável pela manutenção e execução do software necessário ao Plano de Contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NDA – TI;
    - NPD – TI;

g) Operação
- Grupo responsável pela operacionalização do hardware e software necessários ao Plano de contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NDA – TI;
    - NPD – TI.

h) Comunicações
- Coordenará e executará os procedimentos necessários à manutenção e operacionalização do Plano de Contingência;
- Este grupo é composto por membros das seguintes áreas:
    - NDA-TI;
    - NPD-TI;
    - Setor de telefonia/Proinfra/UFSC.

i) Microinformática
- Este grupo é responsável pela execução dos procedimentos necessários à manutenção e operacionalização da estrutura de microinformática necessária ao Plano de Contingência;
- Entende-se microinformática as seguintes atividades de manutenção, suporte de equipamentos operacionais tal como, desktops, notebooks, PDAs, Smartphones e dispositivos portáteis;
- Este grupo é composto por membros das seguintes áreas:
    - NDA-TI;
    - NPD-TI;
    - Operação;

3. Responsabilidades

Comitê de Segurança

- **Permanentes**
  - Coordenar as atividades dos demais grupos;
  - Revisar periodicamente o plano de contingência;
  - Distribuir cópia do plano de contingência aos demais grupos;
  - Informar aos demais grupos o status do plano de contingência;
  - Organizar e coordenar a execução dos testes do plano de contingência;
  - Dar apoio a todos os grupos envolvidos no plano de contingência.
- **Na ativação da contingência**
  - Registrar os incidentes;
  - Coordenar a ativação do plano de contingência;
  - Coordenar as atividades dos demais grupos.
- **Durante a contingência**
  - Coordenar as atividades dos demais grupos;
  - Resolver conflitos entre os grupos;
  - Solucionar problemas imprevistos.
- **Retorno à normalidade**
  - Coordenar as atividades de retorno à normalidade;
  - Registrar as situações não previstas

Área de Pesquisa

- **Permanentes**
  - Registrar as características de cada pesquisa desenvolvida no EQA;
  - Definir o grau de importância e criticidade de cada pesquisa;
  - Registrar os recursos necessários à cada pesquisa;
  - Manter o Comitê de Segurança informado sobre cada pesquisa em desenvolvimento;
  - Informar ao Comitê de Segurança qual é a estrutura mínima necessária para cada pesquisa em desenvolvimento.
- **Na ativação da contingência**
  - Seguir as orientações do Comitê de Segurança;
  - Ativar o plano de contingência, caso o incidente esteja relacionado à sua área de responsabilidade.
- **Durante a contingência**
  - Executar o plano de contingência, caso o incidente esteja relacionado à sua área de responsabilidade;
  - Monitorar as atividades em execução sob sua responsabilidade;
  - Manter os demais grupos informados quanto às etapas executadas.
- **Retorno à normalidade**
  - Preparar e ativar a estrutura de retorno à normalidade, caso o incidente ocorrido esteja relacionado à sua área de responsabilidade;
  - Relatar ao Comitê de Segurança as situações que não foram previstas no plano de contingência.

Apoio Administrativo

- **Permanentes**
  - Manter atualizados os meios de comunicação dos envolvidos no plano de contingência, tais como: números de telefone (celular e fixo), endereços (de e-mail, residencial e profissional);
  - Divulgar, aos membros do plano de contingência, os meios de comunicação de todos os envolvidos;
  - Manter reserva de recursos financeiros suficiente para operacionalizar o plano de contingência.
- **Na ativação da contingência**
  - Seguir as orientações do Comitê de Segurança;
  - Ativar o plano de contingência, caso o incidente esteja relacionado à sua área de responsabilidade;
  - Fornecer local apropriado para instalação do Centro de Operações do Plano de Contingência;
  - Prover o local do Centro de Operações com meios de comunicação adequados às necessidades do grupo;
- **Durante a contingência**
  - Fornecer material de escritório básico (lápis, caneta, papel, mesa, cadeira e armário), para atividades não tecnológicas;
  - Fornecer meios de transporte adequados às necessidades de locomoção dos membros do grupo.
- **Retorno à normalidade**
  - Apoiar administrativamente os demais grupos nas rotinas de retorno à normalidade.

Aplicativos

- **Permanentes**
  - Manter atualizadas todas as rotinas que compõem o plano de contingência;
  - Desenvolver as rotinas destinadas aos serviços críticos;
  - Manter atualizadas, e em lugar seguro, cópias da documentação dos sistemas de aplicativos de serviços críticos;
  - Prever e desenvolver rotinas para atender a todas as condições de retorno à normalidade, para as rotinas de contingência.
- **Na ativação da contingência**
  - Dar apoio necessário para a ativação do plano de contingência.
- **Durante a contingência**
  - Dar apoio e auxílio técnico para a solução de problemas imprevistos;
  - Efetuar as correções necessárias nos sistemas de aplicativos de contingência.
- **Retorno à normalidade**
  - Apoiar tecnicamente os demais grupos nas rotinas de retorno à normalidade.

Hardware

- **Permanentes**
  - Manter atualizada e informar, aos grupos que participam do plano de contingência, a relação dos equipamentos existentes e a situação de cada um;
  - Pesquisar e providenciar um centro de processamento de dados alternativo com as características mínimas necessárias à execução do plano de contingência;
  - Analisar e propor as melhores alternativas de contingência para o hardware utilizado pelos pesquisadores do EQA.
- **Na ativação da contingência**
  - Comunicar aos grupos que participam do plano de contingência quaisquer avarias que possam afetar as pesquisas em desenvolvimento no EQA, fornecendo a previsão para correção do problema;
  - Efetuar os contatos com os fornecedores de peças e suprimentos para garantir a reposição dos componentes danificados.
- **Durante a contingência**
  - Providenciar o reparo/substituição da instalação/hardware danificado;
  - Providenciar o(s) equipamento(s) alternativo(s) e ativá-lo(s);
  - Contatar os fornecedores visando a reposição das peças e suprimentos danificados.
- **Retorno à normalidade**
  - Concluir a correção ao(s) equipamento(s) danificado(s) e comunicar a todos os grupos que participam do plano de contingência, visando o retorno à normalidade.

Software

- **Permanentes**
  - Manter atualizada e informar, aos grupos que participam do pano de contingência, a relação de todos os softwares disponíveis na instalação, identificando sua utilização e usuários principais;
  - Instalar e manter atualizado(s) equipamento(s) alternativo(s), com o(s) sistema(s) operacional(is) utilizado(s) pelos pesquisadores do EQA;
  - Planejar e colocar em prática o esquema de cópias de contingência para todos os softwares críticos que serão necessários ao plano de contingência.
- **Na ativação da contingência**
  - Ativar o(s) hardware(s) com o(s) sistema(s) operacional(is) necessário(s) ao plano de contingência;
  - Instalar o(s) software(s) crítico(s) necessário(s) ao plano de contingência.
- **Durante a contingência**
  - Apoiar e resolver situações imprevistas relacionadas ao(s) software(s) crítico(s).
- **Retorno à normalidade**
  - Desinstalar o(s) software(s) utilizado(s) na ativação da contingência;
  - Relatar as situações imprevistas e as soluções adotadas, visando aprimorar o plano de contingência.

Operação

- **Permanentes**
  - Manter atualizado o esquema de operacionalização dos programas de pesquisa críticos do EQA;
  - Providenciar local livre de riscos e guardar as cópias de segurança dos sistemas e aplicativos necessários ao plano de contingência;
  - Estabelecer procedimentos detalhados de operação para ser utilizado durante o plano de contingência;
  - Providenciar local alternativo para entrada dos dados, durante a contingência;
  - Desenvolver procedimentos alternativos para o caso de panes parciais do servidor que atende os projetos de pesquisa;
- **Na ativação da contingência**
  - Comunicar ao grupo responsável pelo hardware, ocorrência de pane que possa configurar uma emergência.
- **Durante a contingência**
  - Operar o(s) sistema(s) crítico(s) da área de pesquisa no equipamento alternativo designado pelo Comitê de Segurança;
  - Manter o esquema de cópia de segurança para os arquivos e sistemas que estão funcionando em regime de contingência.
- **Retorno à normalidade**
  - Operar a(s) rotina(s) introduzirá os dados no sistema e que foram coletados na forma alternativa.

Comunicações

- **Permanentes**
  - Manter atualizada e informar, aos grupos que participam do pano de contingência, a relação e características dos meios de comunicação disponíveis na instalação, identificando sua utilização e usuários principais;
  - Instalar e manter atualizado(s) as características e configuração do(s) equipamento(s) alternativo(s) comunicações, que serão utilizados durante o plano de contingência;
  - Analisar e propor melhorias alternativas para os equipamentos de comunicação que apresentarem falha ou fadiga;
  - Instalar e testar os equipamentos de comunicação alternativos que serão utilizados no plano de contingência.
- **Na ativação da contingência**
  - Comunicar aos grupos que participam do plano de contingência quaisquer avarias nos equipamentos de comunicação que possam afetar as pesquisas em desenvolvimento no EQA, fornecendo a previsão para correção do problema;
  - Efetuar os contatos com os fornecedores de peças e suprimentos para garantir a reposição dos componentes ou equipamentos danificados.
- **Durante a contingência**
  - Ativar os equipamentos de comunicação alternativos, nas áreas mais sensíveis do EQA, visando não interromper completamente as comunicações;
  - Monitorar os equipamentos alternativos, para que as comunicações não sejam completamente interrompidas;

- **Retorno à normalidade**
  - Relacionar os equipamentos danificados e quais peças serão necessárias repor;
  - Identificar e relatar situações não previstas no plano de contingência;

Microinformática

- **Permanentes**
  - Manter atualizada e informar, aos grupos que participam do plano de contingência, a relação dos equipamentos existentes e seus respectivos usuários;
- **Na ativação da contingência**
  - Comunicar aos grupos do plano de contingência quaisquer avarias o mal funcionamento dos equipamentos de comunicação.
- **Durante a contingência**
  - Identificar e substituir os equipamentos de microinformática que possam prejudicar os projetos de pesquisa do EQA.
- **Retorno à normalidade**
  - Relatar ao Comitê de Segurança os equipamentos que apresentaram pane durante o plano de contingência;
  - Tentar recuperar e por em produção, os equipamentos que apresentaram pane.

4. Plano de ação

Controles a ser mantidos:

- **Equipamentos**
  - Manter atualizado o inventário dos equipamentos críticos que podem, em caso de falha, prejudicar as atividades diárias do EQA;
  - Testar periodicamente os equipamentos alternativos que serão utilizados em caso de falha dos equipamentos principais;
- **Softwares**
  - Manter atualizado o inventário dos softwares críticos, incluindo os principais usuários;
  - Desenvolver e manter um esquema de atualização periódica dos softwares críticos alternativos.
- **Infraestrutura de apoio**
  - Verificar periodicamente o local alternativo escolhido para continuar o desenvolvimento das pesquisas do EQA;
- **Aplicativos**
  - Manter atualizado o inventário dos aplicativos críticos e seus respectivos usuários.
- **Treinamento**
  - Executar periodicamente o programa de simulações periódicas para teste de plano de contingência;
- **Documentação**
  - Desenvolver e manter esquema de atualização das documentações dos softwares e sistemas críticos.

Procedimentos de retorno

Na tabela abaixo estão os procedimentos de retorno que deverão ser executados com relação aos principais eventos identificados no levantamento de riscos, e que possibilitarão o retorno à normalidade.

Evento:	Perda de informações.
Descrição:	Ocorre quando a informação é perdida, devido a destruição indevida ou intencional, para provocar dano ao EQA.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Se o documento que será recuperado for magnético, restaurar o arquivo de backup. Se o documento a ser recuperado não for magnético, consultar o(s) autor(es) para definir a melhor maneira de reconstruí-lo.
RTO:	6 horas.
RPO:	1 dia.
Evento:	Interrupção do acesso à rede.
Descrição:	Ocorre quando o acesso à rede (LAN ou WAN) está indisponível, devido à falha na infraestrutura de cabeamento ou mal funcionamento de equipamento de conexão da rede do EQA.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Dependendo da gravidade do incidente, será ativada uma das seguintes opções: III Ponto de acesso sem fio; IV Modem dial-up; V Conexão Wi-Fi; VI Ativar o protocolo HSRP (Hot Standby Router Protocol) nos roteadores, para que sejam criadas rotas redundantes entre os roteadores do EQA; VII Ativar o protocolo Spanning Tree (STP) nos switches do EQA, para solucionar eventuais casos de loop; VIII Trocar os path cords e cabos de distribuição por cabos testados e certificados.
RTO:	30 minutos.
RPO:	N/A.
Evento:	Ataque de negação de serviço de grande impacto.

Descrição:	Ocorre quando é detectado um ataque de negação de serviço (DoS ou DDoS), destinado a interromper ou prejudicar pelo menos um dos seguintes serviços: DNS, HTTP, Web, Webmail, rede wireless.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Identifica o atacante, através dos logs de monitoração e o inclui na lista negra do firewall, para posterior bloqueio.
RTO:	15 minutos.
RPO:	1 dia.
Evento:	Vandalismo contra equipamento do EQA.
Descrição:	Ocorre quando pessoa mal intencionada desliga ou danifica equipamento do EQA (microcomputador, switch, impressora), objetivando gerar prejuízo a determinada atividade de negócio.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Dependendo da gravidade do incidente, será ativada uma das seguintes opções: a) No caso de desligamento, verificar como o fato ocorreu e, se possível, ligá-lo novamente. Avaliar se houve perda de informação e, caso necessário, recuperá-la através do backup. b) No caso de dano a equipamento, verificar se há condição de ligá-lo novamente. Caso não seja possível, utilizar outro equipamento semelhante, remanejado de algum setor cuja atividade possa ser interrompida, até que o equipamento danificado seja recuperado ou substituído.
RTO:	1 dia.
RPO:	1 dia.
Evento:	Impossibilidade de acesso ao conhecimento tácito.
Descrição:	Ocorre quando algum membro do EQA retém conhecimento tácito, devido à “concentração da informação”, e o acesso a este conhecimento fica indisponível devido à ausência desta pessoa.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente;

	Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Dependendo da gravidade do incidente, será ativada uma das seguintes opções: a) Excetuando o caso de falecimento, buscar estabelecer contato com a pessoa que detêm o conhecimento, através dos meios de comunicação disponíveis, tais como telefone (celular ou fixo), correio eletrônico, telegrama, carta, ou através de pessoa de contato. b) No caso de falecimento, designar duas pessoas da equipe para serem treinadas, através das informações existentes e desenvolvendo o próprio conhecimento tácito.
RTO:	1 dia.
RPO:	N/A.
Evento:	Falta de energia (blackout).
Descrição:	Ocorre quando há interrupção do fornecimento de energia elétrica pela operadora local, independente do motivo.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: O fornecimento de energia elétrica alternativa pode ser originado de duas fontes, dependendo do tempo de duração do evento. A primeira fonte, que entrará em ação imediatamente, será o nobreak instalado ao equipamento de rede indispensável à manutenção de serviço ou atividade. Preferencialmente serão utilizados nobreaks inteligentes, que possam ser monitorados pelo equipamento ao qual este está ligado. Na falta da segunda fonte de energia, o equipamento será desligado normalmente, evitando perda de dados. A segunda fonte, que será acionada momentos após a primeira entrar em ação, será o gerador (movido a diesel, gás ou outro combustível), e fornecerá energia aos setores do EQA que não podem ter suas atividades interrompidas. Desta forma é evitada a paralisação no negócio e racionalizado o fornecimento de energia elétrica.
RTO:	30 minutos.
RPO:	30 minutos.
Evento:	Desastre natural.
Descrição:	Ocorre quando um desastre natural, previsto ou não, interrompe ou inviabiliza alguma atividade vital do EQA. Os principais desastres naturais que podem ocorrer são: inundação, granizo, furação, tornado, terremoto.

Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Avalia superficialmente a situação e designa o técnico que executará a recuperação; Comitê de segurança: Transferir os processos de pesquisa do EQA para local alternativo, conforme o caso: a) serviços de rede serão transferidos para outros equipamentos, provisoriamente; b) acesso a documentos digitais serão transferidos para outros servidores, através da restauração de arquivos de backup; c) atividades administrativas, acadêmicas ou de pesquisa serão transferidas para local alternativo.
RTO:	1 dia.
RPO:	1 dia.
Evento:	Sinistro ocasionado pelo fogo.
Descrição:	Ocorre quando instalações ou equipamentos são danificados ou destruídos por incêndio, independente de ser acidental ou intencional.
Contingência:	Usuário final: Comunica ao Coordenador da pesquisa o incidente; Coordenador da pesquisa: Comunica o fato à Comissão de segurança; Comitê de segurança: Registra o incidente; Comitê de segurança: Comunica o incidente à Brigada de incêndio, que acionará os procedimentos específicos de combate a incêndio; Comitê de segurança: O processo de negócio afetado pelo incêndio será transferido para outro equipamento ou local. Comitê de segurança: Recupera as informações necessárias para o funcionamento do processo de negócio, através da restauração de arquivos de backup.
RTO:	1 minuto.
RPO:	1 dia.
Evento:	Furto de informação.
Descrição:	Ocorre quando uma informação sensível é furtada, independente se o acesso é físico ou lógico.
Contingência:	Se houve subtração da informação, esta será restaurada através do arquivo de backup.
RTO:	6 horas.
RPO:	1 dia.
Evento:	Indisponibilidade de suporte técnico.
Descrição:	Ocorre quando há indisponibilidade de técnicos para prestar suporte a equipamentos e serviços de informática, devido a alta

	rotatividade da equipe de TI.
Contingência:	Os serviços de manutenção deverão ser priorizados, levando-se em consideração a relevância e a urgência do serviço. Desta forma o atendimento prestado pelo suporte técnico será otimizado e os serviços vitais preservados.
RTO:	1 hora.
RPO:	1 hora.
Evento:	Apropriação indevida da informação.
Descrição:	Ocorre quando pessoa mal intencionada se apropria de informação sensível ou vital para o EQA, caracterizando principalmente espionagem industrial, independente se a informação é subtraída ou o acesso é físico ou lógico.
Contingência:	Se houve subtração da informação, esta será restaurada através do arquivo de backup.
RTO:	6 horas.
RPO:	1 dia.
Evento:	Senha fraca utilizada em equipamento servidor.
Descrição:	Ocorre quando é verificada a utilização de senha de fácil descoberta em equipamento servidor.
Contingência:	Trocar a senha, utilizando regra de construção de senha forte.
RTO:	1 hora.
RPO:	N/A.
Evento:	Instalação não autorizada de ativos de rede.
Descrição:	Ocorre quando é detectada instalação não autorizada de ativo de rede (switch, hub ou ponto de acesso wireless).
Contingência:	Não há necessidade de procedimento de contingência, uma vez que nenhum processo de negócio será interrompido. Entretanto, a instalação será desfeita e o ativo de rede confiscado.
RTO:	N/A.
RPO:	N/A.

5. Operacionalização do Plano

Manuais de Contingência

a) Quem mantém e atualiza:
   - Secretariado das pesquisas – (Apêndice IV);
   - Equipe de TI (NDA e NPD) – (Apêndice IV).

b) Quem recebe cópias parciais/totais:
   - Coordenadores das pesquisas – (Apêndice IV);
   - Secretariado das pesquisas – (Apêndice IV);
   - Equipe de TI – (Apêndice IV).

c) Periodicidade de atualização
   - Este Plano de Contingência será atualizado pelos grupos envolvidos a cada seis meses e revisado a cada ano.

d) Fontes de informação
   - WEB
   - Normas da ABNT
   - Manuais
   - Artigos/Paper
   - Descrição dos equipamentos
   - CPU´s
   - Storage
   - Ativos de rede

e) Descrição dos softwares necessários
   - Sistemas operacionais:
     - Microsoft Windows XP
     - Ubuntu
     - Brlix
   - Aplicativos
     - Microsoft Office
     - Broffice
     - Matlab
     - Adobe acrobat
     - Matemática
     - Estatística

f) Descrição dos aplicativos necessários
   - CFX
   - Autocad
   - Pro-engineer

Relação de Pessoal

A relação de todas as pessoas envolvidas neste Plano de Contingência pode ser encontrada nos seguintes documentos, que integram este Plano de Contingência:

- Apêndice IV: Relação de responsáveis por áreas;

- Apêndice V: Relação dos Fornecedores.

Relação dos equipamentos e softwares

b) Hardware do CPD central
   - Tipo: CPU – DELL
   - Função: Servidor de autenticação CFX (Aplicativo)
   - Modelo: Dell Enterprise
   - Série 768952-yxk
   - Descrição: Processador quadcore 2.8 GHZ
   - Capacidade do disco rígido: 500GB
   - Capacidade de memória RAM: 8GB
   - Consumo de energia: 1000 watts/hora
   - Consumo ar-condicionado: 0,5 BTU´s/hora
   - Quantidade: 02
   - Área necessária: 10 m²
   - Data de instalação: jan/09
   - Atualização técnica efetuada.

c) Equipamentos e rede de teleprocessamento
   - Roteadores Cisco
   - Switch de camada 3
   - Switch de camada 2
   - Modems Telex
   - Conexão Internet da Pop-SC
   - Sistema VOIP da RNP (Rede Nacional de Pesquisa)

d) Equipamentos auxiliares
   - Energia elétrica
     - no-break e banco de baterias
   - Ar-condicionado
     - Central e individual tipo split
   - Extinção de incêndio
     - Por padrão são adotados extintores portáteis
   - Iluminação de emergência
     - Iluminação de emergência alimentada pelo banco de baterias

e) Software
   - Software básico:
     - Ubuntu 9.04;
     - Windows XP SP3;
     - BRlix 1.2;
     - Open Suse 9.12;
   - Software de apoio
     - Microsoft Office;
     - BrOffice.org;
     - OpenOffice;
     - Adobe Acrobat,
     - CFX;

    - Pro-engineer
  - Software de comunicação
    - Browsers (IE8.0, Firefox 3.0, Opera 10);
    - software fone (x-lite);
    - SMS messenger

f) Microcomputadores
  - CPU padrão desktop:
    - Processador: AMD ou Intel 1,5 a 2 Ghz;
    - Memória RAM: 512 Mb;
    - Disco rígido: 100 Mb;
    - Sistema operacional: Windows XP ou Ubuntu;
    - Aplicativos: MS Office ou BrOffice.org, Statistica;
    - Todos com conexão a internet.
  - CPU padrão Servidor:
    - Processador: Intel 2 a 3 Ghz;
    - Memória RAM: de 2 a 4 Gb;
    - Disco rígido: de 500 Gb a 1 Tb;
    - Sistema operacional: Windows Server ou Distribuição Linux Server 64 bits;
    - Aplicativos: Específicos ao serviço, por exemplo o aplicativo CFX, Autocad etc.;
    - Todos com conexão internet

6. Relação de pessoal de informática

- Consulte o Apêndice IV.

7. Relação de pessoal de apoio técnico

- Consulte o Apêndice IV.

8. Relação de fornecedores

- Consulte o Apêndice V.

9. Relação de aplicativos

- Sistemas Operacionais:
  - Ubuntu 9.04;
  - Windows XP SP3;
  - BRlix 1.2;
  - OpenSuse 9.12
- Aplicativos:
  - Microsoft Office;
  - BrOffice.org;
  - OpenOffice;
  - Adobe Acrobat;
  - CFX;

    - Pro-engineer;
- Software de comunicação:
    - Browsers (Internet Explorer 8.0, Firefox 3.0, Opera 10);
    - software fone (x-lite);
    - SMS Messenger.

10. Apêndices

- Apêndice IV: Relação de responsáveis por áreas de atuação;
- Apêndice V: Relação de fornecedores.

11. Referências Bibliográficas

CARUSO, Carlos A. A.; STEFFEN, Flávio Deny. **Segurança em informática e de informações.** 3ª edição, São Paulo: Editora SENAC São Paulo, 2006.

12. Equipe de desenvolvimento do Plano de Contingência

- Jorge Antônio Coelho de Sousa
- Roberto Rivelino Dias
- Rossano Cancelier
- Sandro dos Santos Souza

Apêndice IV - Relação de responsáveis por áreas

Nome	Telefone convencional	Telefone residencial	Telefone residencial	e-mail	Cargo	Lotação/Curso/Pesquisa
					Coordenadores dos cursos CPGENQ/CPGEA	
					Coordenadores de pesquisa	
					Supervisor NDA	
					Secretária do grupo de pesquisas LCP/EQA - Laboratório de controle de processos	Equipe de apoio técnico
					Supervisor NPD	
Data última atualização:						

Apêndice V - Relação de fornecedores

Nome	Contato	Telefone convencional	Telefone residencial	e-mail	Objeto fornecido	Usuário
Data última atualização:						

ANEXOS

Anexo I – Ofício do SENAC solicitando autorização para pesquisar o EQA

senac

OFÍCIO

Os alunos da pós-graduação em Segurança da Informação da Faculdade Senac: **Jorge Antonio Coelho de Souza**, CPF [redacted] – Matrícula Nº 150830; **Roberto Rivelino Dias**, CPF [redacted] – Matrícula Nº 100022696; **Rossano Cancelier**, CPF [redacted] – Matrícula Nº 110007933 e **Sandro dos Santos Souza**, CPF [redacted] – Matrícula Nº 110019959 (funcionário do EQA – UFSC) solicitam, desta conceituada instituição, a permissão de acesso ao Departamento de Engenharia Química e de Alimentos a fim de buscarem informações para conclusão do trabalho de especialização do curso.

RECEBIDO
Em 10/08/09
Assinatura

Secretária Acadêmica

03.603.739/0007 - 71
Serviço Nacional de Aprendizagem
Comercial - SENAC
RUA SILVA JARDIM 360
PRAINHA - CE 88020-200
FLORIANÓPOLIS - SC

Anexo II - Portaria 337/GR/2007

UNIVERSIDADE FEDERAL DE SANTA CATARINA
GABINETE DO REITOR
PORTARIAS

Florianópolis, 13 de abril de 2007. **PORTARIA N° 337/GR/2007.**

A Pró-Reitora de Pesquisa da Universidade Federal de Santa Catarina, no exercício da Reitoria, no uso de suas atribuições estatutárias e regimentais, tendo em vista o disposto no art. 16 da Lei n° 10.9 73/2004, que estabelece medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo com vistas à capacitação e ao alcance da autonomia tecnológica e ao desenvolvimento industrial do País, nos termos dos artigos 218 e 219 da Constituição Federal, e no art. 29 do Decreto n° 5.563/2005, que a regulamenta,

RESOLVE:

Art. 1º Criar o Núcleo de Inovação Tecnológica (NIT) da Universidade Federal de Santa Catarina como instrumento de coordenação das medidas de incentivo à inovação e à pesquisa científica e tecnológica para o ambiente produtivo, das atividades relacionadas à criação, adaptação, absorção e transferência de tecnologia e à propriedade intelectual.

Parágrafo único. O Núcleo de Inovação Tecnológica ficará subordinado administrativamente à Pró-Reitoria de Pesquisa.

Art. 2º Compete ao Núcleo de Inovação Tecnológica, na medida do interesse da Universidade:
I - zelar pela manutenção da política institucional de estímulo à proteção das criações, à inovação, ao licenciamento e outras formas de transferência de tecno10gia;
II - avaliar e classificar os resultados decorrentes de atividades e projetos de pesquisa para o atendimento das disposições da lei de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo;
IX - avaliar os pedidos de adoção de invenção, apresentados por inventor independente;

X - opinar pela conveniência e promover a proteção das criações desenvolvidas no âmbito da Universidade;
V - opinar quanto à conveniência de divulgação das criações desenvolvidas no âmbito da Universidade, passíveis de proteção intelectual;
VI - acompanhar o processamento dos pedidos e a manutenção dos títulos de propriedade intelectual da Universidade;
VII - identificar e incentivar, no ambiente produtivo, oportunidades de realização de projetos de inovação que poderão ser executados em conjunto com a Universidade;
VIII - opinar quanto à celebração de contratos e convênios envolvendo a inovação e a pesquisa científica e tecnológica e que incluam cláusulas de propriedade intelectual e de segredo;
IX - divulgar amplamente os resultados obtidos com os projetos de inovação desenvolvidos no âmbito da Universidade, resguardando o dever de segredo previsto em contratos ou convênios firmados;
X - estabelecer o seu Regimento Interno, a ser aprovado pelo Pró-Reitor de Pesquisa.

Art. 3° A direção do Núcleo de Inovação Tecnológica será exercida, cumulativamente, pelo Diretor do Departamento de Propriedade Intelectual ou pelo Diretor do Departamento de Projetos, indicado pelo Pró-Reitor de Pesquisa e designado pelo Reitor.

Art. 4° O Diretor será responsável pela supervisão de todas as atividades do Núcleo de Inovação Tecnológica.

Art.5° O Núcleo de Inovação Tecnológica poderá usar a marca ou a designação de UFSC INOVAR.

Art. 6° Fica criado o Comitê Consultor *Ad Hoc* para manifestar-se sobre projetos, propriedade intelectual, transferência de tecnologia e incentivo à inovação da Universidade.

§ 1 ° Os consultores *Ad Hoc* serão indicados pelo Diretor do Núcleo de Inovação Tecnológica e designados pelo Pró-Reitor de Pesquisa.

§ 2° As funções de membro do Comitê Consultor *Ad Hoc* serão consideradas missão de serviço relevante.

Art. 7° Esta portaria normativa entrará em vigor na data da sua publicação no Boletim Oficial da Universidade.

Profª. Thereza Christina Monteiro de Lima Nogueira

*Fonte: (*www.propesquisa.ufsc.br/arquivos/Portaria_337_GR_2007.pdf*)*

Anexo III - Termos de Confidencialidade (Mestrandos e Doutorandos)

TERMO DE CONFIDENCIALIDADE
DEFESA DE [DISSERTAÇÃO ou TESE] DO PROGRAMA DE [MESTRADO ou DOUTORADO]
[NOME DO CURSO]

[Dissertação do mestrando ou Tese do doutorando]: [NOME POR EXTENSO]
Patente UFSC [a ser requerida ou já requerida]
Título: "-----" [ou outro a ser definido].

Os signatários declaram estar ciente de que a UFSC é detentora de conhecimentos, informações e dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços que são ou poderão ser objeto de proteção por direitos de propriedade intelectual – especialmente o conteúdo da dissertação referida em epígrafe.
CONSIDERANDO que os membros da banca, docentes, pesquisadores, técnicos e estudantes que firmaram este documento tiveram acesso parcial ou total a dissertação e/ou assistiram a sua defesa.
CONSIDERANDO o que dispõe a Resolução n.º 14 do Conselho Universitário da UFSC, 25/6/2002, que os signatários declaram ter conhecimento.
CONSIDERANDO que a Lei nº 9.279, 14/5/1996, que regula direitos e obrigações relativos à propriedade industrial, art. 195, XI e XII, estabelece que comete crime de concorrência desleal quem divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato; também quem divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o item anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; prevendo aplicação de pena de detenção de três meses a um ano ou multa para o infrator.
CONSIDERANDO que a legislação penal e da propriedade intelectual prevê outros delitos que podem ser considerados crimes e que se aplicam também sanções civis de caráter indenizatórias e administrativas, sem prejuízo das penas criminais cabíveis.
CONSIDERANDO que tenho o dever de informar à UFSC sobre qualquer determinação judicial para dar testemunho sobre conhecimentos, informações ou dados a que tiver acesso direto ou indireto na geração de conhecimento mencionado no início.

DECLARAMOS que nos responsabilizamos pela manutenção da confidencialidade dos conhecimentos, informações e dados a que tivemos acesso, e que não os utilizaremos, individual ou coletivamente, total ou parcialmente, em benefício próprio ou de terceiros.
DECLARAMOS o pleno conhecimento das sanções previstas em lei relacionadas à propriedade intelectual no caso de revelar ou usar os conhecimentos, informações e dados, sem a previa autorização por escrito do representante legal da UFSC.

Florianópolis, UFSC, __ de _____ de 200_.

[nome completo – CPF – assinatura]
[assinam todos os membros da banca, suplentes e que assistir]

*Fonte: (*http://www.dit.ufsc.br/index.php?option=com_docman&Itemid=89*)*

Anexo IV - Termo de Confidencialidade (Pesquisadores)

LABORATÓRIO DE [nome do laboratório]

Eu, [nome completo], [solteiro/ casado/ separado], [empregado/ servidor – docente, pesquisador, técnico/ estudante/ prestador de serviço/ avaliador/ auditor ou fiscal], [setor da UFSC], cédula de identidade n° ....., expedida no dia .../.../..., em [local], CPF n° ....., residente na [rua/ avenida, n°, apto, bloco, bairro, CEP, cidade, estado], a seguir "signatário", **declaro**:

Estou ciente de que são e serão tratados como confidenciais os dados, informações e conhecimentos aportados para a execução de projetos, os resultados gerados na execução de projetos, durante e após a sua vigência, bem como todos os assuntos relacionados à pesquisa realizada no Laboratório [nome do laboratório], a seguir **[sigla do laboratório].**

Será considerado, sem limitar-se ao conceito aqui expresso:
DADO: o elemento ou quantidade que servir de base à resolução de um problema; os números de uma amostra que têm as características definidas por um subconjunto do domínio de uma variável aleatória ou não; resultados de exames, testes, ensaios;
INFORMAÇÃO: o conjunto de dados logicamente concatenados para esclarecimentos acerca de procedimento para utilização do conhecimento;
CONHECIMENTO: o saber científico ou tecnológico, domínio teórico e/ou prático, porém referido especificamente ao **Projeto**;
TECNOLÓGICO: o conjunto de instrumentos, métodos e processos específicos; o estudo sistemático das matérias-primas e dos procedimentos e equipamentos técnicos necessários para a transformação das matérias-primas em produto industrial;
PROJETO: o conjunto de atividades visando gerar conhecimento ou informação ou dado, cujo resultado esperado é um produto ou processo novo para aplicar na indústria; poderá ser uma inovação; por isso "confidencial".

§ 1º. A confidencialidade implica na obrigação de não divulgar ou repassar dados, informações e conhecimentos a terceiros não-envolvidos no [sigla do laboratório], sem autorização expressa, por escrito, do coordenador do Laboratório, Prof. Dr. [nome completo], pelo período de 10 (dez) anos, ficando sujeito às sanções das Leis 9.279/96, art. 195, e 9.609/98, art. 12. Na UFSC o Departamento de Inovação Tecnológica é o órgão competente para dar a autorização para divulgação na ausência ou impedimento do Coordenador do [sigla do laboratório].

§ 2º. Não serão tratados como confidenciais os dados, informações e conhecimentos nos limites para o cumprimento dos seguintes atos:
1) quando se tornarem de conhecimento geral pela publicação de pedido de patente ou registro público ou de outra forma que não por meio do signatário;
2) aqueles cuja divulgação se torne necessária:
2.1) para obtenção de autorização governamental para comercialização dos resultados de projeto;
2.2) quando exigida por lei ou quando necessária ao cumprimento de determinação judicial e/ou governamental;
2.3) nos casos previstos nos itens "2.1" [sigla do laboratório] e o Departamento de Inovação Tecnológica e requerer segredo no seu trato judicial e/ou administrativo.

§ 3º. Quando algum resultado de projeto do [sigla do laboratório], ao amparo deste termo, for objeto de tese, dissertação, monografia, trabalho de conclusão de curso, artigo, folheto ou relatório, com o objetivo de evitar a quebra de sigilo, o signatário deverá solicitar ao

Coordenador do [sigla do laboratório] e do Departamento de Inovação Tecnológica da UFSC autorização para a divulgação ou publicação.
1) A solicitação será feita com trinta (30) dias de antecedência e deverá ser respondida no mesmo prazo.
2) Excepcionalmente, poderá haver defesa perante banca ou acesso aos documentos de projeto, mediante assinatura de termo de sigilo, sempre que autorizado pelo Coordenador do [sigla do laboratório] e do Departamento de Inovação Tecnológica da UFSC.

§ 4º. O signatário está ciente de que, somente depois da publicação oficial do órgão competente de patente, de registro ou de outra proteção legal da propriedade intelectual, poderá publicar ou divulgado resultado de projeto, não excedendo a descrição constante dos referidos documentos.

§ 5º. Qualquer exceção à confidencialidade prevista neste termo, somente será possível com a anuência prévia do Coordenador do [sigla do laboratório] e autorização do Departamento de Inovação Tecnológica da UFSC.

§ 6º. O signatário declara conhecer a Resolução nº 014/CUn/UFSC, de 25 de junho de 2002, e que é ou será propriedade da UFSC a criação intelectual desenvolvida no seu âmbito; bem como, ter direito a participação nos ganhos econômicos resultantes da exploração da criação intelectual protegida na proporção fixada no projeto ou de acordo com a contribuição individual para o êxito da criação conjunta nos termos da Resolução. Inclusive aqueles que forem objeto de pedido de proteção da propriedade intelectual (patente, registros, certificado) relacionado ao projeto ou atividades do [sigla do laboratório] até um ano após o meu desligamento da UFSC.

§ 7º. Qualquer demanda que envolver a UFSC será apreciada pelo foro privilegiado da Seção Judiciária de Florianópolis da Justiça Federal do Estado de Santa Catarina

Assim, por considerar válida e eficaz a obrigação unilateral aqui expressa, assino perante as testemunhas abaixo, o presente instrumento, em duas vias de igual teor e forma, uma para a UFSC e outra para mim, para que produza os efeitos legais.

Florianópolis, UFSC, __ de _____ de 200_.

[nome completo – CPF – assinatura]

Testemunhas/Assinatura:
Nome: _____
CPF: _____
Nome: _____
CPF: _____

*Fonte: (*http://www.dit.ufsc.br/index.php?option=com_docman&Itemid=89*)*

Anexo V - Dispositivos legais de caráter Federal

Dispositivo	Mandamento Legal	Aspecto da SI
Constituição Federal, art. 5º, inciso X.	Direito à privacidade.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XII.	Direito à privacidade das comunicações.	Sigilo dos dados telemáticos e das comunicações privadas.
Constituição Federal, art. 5º, inciso XIV.	Resguardo do sigilo profissional em caso de ofício que exige a ampla confidência no interesse de quem confidencia, como advogados, padres, médicos, psicólogos, etc.	Sigilo das informações relacionadas à intimidade ou à vida privada de alguém.
Constituição Federal, art. 5º, inciso XXXIII e art. 37, § 3º, inciso II.	Direito à informação e ao acesso aos registros públicos.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 5º, inciso XXXIV.	Direito de petição e de obtenção de certidões em repartições públicas.	Disponibilidade das informações constantes nos órgãos públicos.
Constituição Federal, art. 23, incisos III e IV.	Dever do Estado de proteger os documentos e obras.	Proteção da integridade, da autenticidade e da disponibilidade das informações pelo Estado.
Constituição Federal, art. 216, § 2º.	Obrigação da Administração Pública de promover a gestão documental.	Proteção da integridade, da autenticidade, da disponibilidade e do sigilo das informações constantes nos órgãos e entidades integrantes da Administração Pública.
Constituição Federal, art. 37, caput.	Vinculação da Administração Pública aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.	Quanto melhor a gestão das informações, mais eficiente será o órgão ou entidade, daí a necessidade de implantação de uma Política de Segurança da Informação.
Constituição Federal, art. 37, § 6º e Código Civil, art. 43.	Responsabilidade objetiva do Estado e das pessoas de direito privado prestadoras de serviços públicos pelos danos causados a terceiros, assegurado o direito de	Responsabilidade objetiva do Estado por dano decorrente da má gestão das informações pelos órgãos e entidades da Administração Pública

Dispositivo	Mandamento Legal	Aspecto da SI
	regresso contra o responsável nos casos de dolo ou culpa.	e pessoas de direito privado prestadoras de serviços públicos.
Constituição Federal, art. 37, § 7º.	Lei disporá sobre os requisitos e as restrições ao ocupante de cargo ou emprego da administração direta e indireta que possibilite o acesso a informações privilegiadas.	Necessidade de regulamentação do acesso a informações privilegiadas.
Consolidação das Leis do Trabalho – CLT, art. 482, alínea g.	Rescisão de contrato de trabalho de empregado que viola segredo da empresa.	Proteção das informações sigilosas acessadas no exercício de emprego público (empresas públicas e sociedades de economia mista).
Código de Conduta da Alta Administração, art. 5º, § 4º.	Caráter sigiloso das informações pertinentes à situação patrimonial da autoridade pública.	Sigilo das informações fiscais e tributárias das autoridades públicas (sigilo perante terceiros e não em face da Administração Pública)..
Código de Conduta da Alta Administração, art.14, inciso II.	Proibição da autoridade pública de prestar consultoria valendo-se de informações não divulgadas publicamente a respeito de programas ou políticas do órgão ou da entidade da Administração Pública Federal a que esteve vinculado ou com que tenha tido relacionamento direto e relevante nos seis meses anteriores ao término do exercício de função pública.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “h” do inciso XV da Seção II.	Proibição de alteração de documentos que devam ser encaminhados para providências.	Proteção da integridade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “l” do inciso XV da Seção II.	Proibição de retirar da repartição documento ou qualquer outro bem.	Proteção da disponibilidade das informações públicas.

Dispositivo	Mandamento Legal	Aspecto da SI
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso X da Seção I.	Deixar o servidor público ou qualquer pessoa à espera de solução que compete ao setor em que exerça suas funções, permitindo a formação de longas filas, ou qualquer outra espécie de atraso na prestação do serviço, não caracteriza apenas atitude contra a ética ou ato de desumanidade, mas principalmente grave dano moral aos usuários dos serviços públicos.	Proteção da disponibilidade das informações públicas.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso VII da Seção I.	Obrigação moral de conferir publicidade aos atos administrativos, salvo os sigilosos.	Proteção da disponibilidade das informações públicas e garantia da publicidade das informações de interesse da coletividade.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), inciso IX da Seção I.	Causar dano a qualquer bem pertencente ao patrimônio público, deteriorando-o, por descuido ou má vontade, não constitui apenas uma ofensa ao equipamento e às instalações ou ao Estado, mas a todos os cidadãos.	Proteção da integridade do patrimônio público, a exemplo de equipamentos, materiais, áreas e instalações.
Decreto nº 1.171/94 (Código de Ética do Servidor Público), alínea “e” do inciso XIV da Seção II.	Dever de aperfeiçoar o processo de comunicação com os usuários para bem servi-los.	Disponibilidade das comunicações.
Código de Propriedade Industrial, art. 75.	O pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso.	Sigilo das patentes de interesse da defesa nacional.
Código de Defesa do Consumidor, arts. 43 e 44.	Direito de acesso do consumidor às suas informações pessoais arquivadas em bancos de dados e direito de retificação das informações incorretas.	Garantia da integridade e disponibilidade das informações dos consumidores arquivadas em bancos de dados.
Código Penal, art. 151.	Pena de detenção de um a seis meses ou multa por crime de violação de	Proteção do sigilo, integridade e disponibilidade das

Dispositivo	Mandamento Legal	Aspecto da SI
	correspondência fechada dirigida a outrem, sonegação ou destruição de correspondência, e violação de comunicação telegráfica, radioelétrica ou telefônica.	informações de caráter pessoal veiculadas através dos meios de comunicação.
Código Penal, art. 152.	Pena de detenção de três meses a dois anos pelo crime de desvio, sonegação, subtração, supressão ou revelação de conteúdo de correspondência comercial, abusando da condição de sócio ou empregado.	Proteção do sigilo e da disponibilidade das informações dos estabelecimentos comerciais.
Código Penal, art. 153.	Pena de 1 a 4 anos e multa por crime de divulgação de documento confidencial contido ou não nos sistemas ou bancos de dados da Administração Pública.	Proteção do sigilo das informações classificadas constantes nos sistemas ou bancos de dados da Administração Pública.
Código Penal, art. 154.	Pena de três meses a um ano, ou multa por crime de violação de segredo profissional.	Proteção do sigilo das informações conhecidas em razão de função, ministério, ofício ou profissão.
Código Penal, art. 184, § 3º.	Pena de dois a quatro anos por crime de violação de direito autoral mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema.	Proteção da autenticidade.
Código Penal, art. 297.	Pena de dois a seis anos, e multa por crime de falsificação de documento público.	Proteção da integridade e autenticidade dos documentos públicos.
Código Penal, art. 298.	Pena de um a cinco anos, e multa por crime de falsificação de documento particular.	Proteção da integridade e autenticidade dos documentos particulares.
Código Penal, art. 305.	Pena de 2 a 6 anos e multa por crime de supressão, destruição ou ocultação de documento público ou particular.	Proteção da disponibilidade e integridade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 307.	Pena de três meses a um ano, ou multa por crime de falsa identidade.	Proteção da autenticidade.

Dispositivo	Mandamento Legal	Aspecto da SI
Código Penal, art. 313-A.	Pena de 2 a 12 anos e multa por crime de inserção de dados falsos em sistema informatizado ou banco de dados da Administração Pública, alteração ou exclusão de dados corretos.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 313-B.	Pena de 3 meses a 2 anos e multa por crime de modificação ou alteração não autorizada de sistemas de informações.	Proteção da integridade e disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 314.	Pena de um a quatro anos por crime de extravio, sonegação ou inutilização de livro ou documento de que tem a guarda em razão do cargo.	Proteção da disponibilidade das informações constantes nos órgãos e entidades públicos.
Código Penal, art. 325.	Pena de seis meses a dois anos, ou multa por crime de violação de sigilo funcional.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Código Processo Penal, art. 20.	Sigilo do inquérito policial	Proteção de informações sigilosas.
Código Processo Penal, art. 207.	Proibição de depor das pessoas que, em razão de função, ministério, ofício ou profissão, devam guardar segredo, salvo se, desobrigadas pela parte interessada, quiserem dar o seu testemunho.	Proteção do sigilo profissional.
Código Processo Penal, art. 745.	Sigilo do processo de reabilitação do condenado.	Proteção de informações sigilosas relacionadas ao condenado.
Código Tributário Nacional, art. 198.	Proibição de divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades.	Proteção do sigilo fiscal.
Código de Processo Civil, art.	Direito da parte de guardar sigilo profissional.	Proteção da privacidade de seus clientes.

Dispositivo	Mandamento Legal	Aspecto da SI
347, inciso II c/c art.363, inciso IV.		
Código de Processo Civil, art. 406, inciso II c/c art.414, § 2º.	Direito da testemunha de guardar sigilo profissional.	Proteção da privacidade de seus clientes.
Lei nº 6.538/78, art. 41.	Pena de detenção de três meses a um ano, ou multa por violação de sigilo profissional por funcionário do serviço postal.	Proteção da privacidade de correspondência.
Lei nº 7.170/83, art. 13.	Pena de três a quinze anos por crime espionagem ou divulgação de informações sigilosas a grupo estrangeiro, ou a organização ou grupo de existência ilegal.	Proteção das informações sigilosas relacionadas à segurança nacional
Lei nº 7.232/84, art. 2o, inciso VIII.	Exigência de mecanismos e instrumentos legais e técnicos para a proteção do sigilo dos dados informatizados armazenados, processados e veiculados, do interesse da privacidade e de segurança das pessoas físicas e jurídicas, privadas e públicas.	Sigilo dos dados relacionados à intimidade, vida privada e honra, especialmente dos dados armazenados através de recursos informáticos.
Lei nº 7.492/86, art. 18.	Pena de reclusão de 1 a 4 anos e multa por crime de violação de sigilo bancário.	Proteção das informações sigilosas no âmbito das instituições financeiras ou integrantes do sistema de distribuição de títulos mobiliários.
Lei nº 8.027/90, artigo 5º, inciso I.	Pena de demissão para o servidor que se valer ou permitir dolosamente que terceiros tirem proveito de informação obtida em função do cargo, para lograr, proveito pessoal ou de outrem.	Proteção das informações privilegiadas produzidas ou acessadas no exercício de cargo ou função pública.
Lei nº 8.027/90, artigo 5º, parágrafo único, inciso V.	Pena de demissão para o servidor que revelar segredo de que teve conhecimento em função do cargo ou emprego.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei nº 8.112/90, art. 116, inciso VIII.	Dever do servidor de guardar sigilo sobre assunto da	Sigilo das informações produzidas ou

Dispositivo	Mandamento Legal	Aspecto da SI
	repartição.	conhecidas no exercício de cargo ou função pública.
Lei nº 8.112/90, art. 132, inciso IX.	Pena de demissão para o servidor que revelar segredo do qual se apropriou em razão do cargo ou função pública.	Proteção das informações sigilosas acessadas no exercício de cargo ou função pública.
Lei nº 8.137/90, art. 3º, inciso I.	Constitui crime funcional contra a ordem tributária punido com pena de 3 a 8 anos e multa extraviar livro oficial, processo fiscal ou qualquer documento, de que tenha a guarda em razão da função; sonegá-lo, ou inutilizá-lo, total ou parcialmente, acarretando pagamento indevido ou inexato de tributo ou contribuição social.	Proteção da disponibilidade de informações para manutenção da ordem tributária.
Lei nº 8.429/92, art.11, incisos III, IV e VII..	Constitui ato de improbidade administrativa revelar fato ou circunstância de que tem ciência em razão das atribuições e que deva permanecer em segredo; negar publicidade aos atos oficiais; e revelar ou permitir que chegue ao conhecimento de terceiro, antes da respectiva divulgação oficial, teor de medida política ou econômica capaz de afetar o preço de mercadoria, bem ou serviço.	Proteção das informações sigilosas acessadas no exercício de cargo, função ou emprego público, bem como garantia de publicidade das informações de interesse coletivo ou geral que devem ser divulgadas por ato oficial.
Lei nº 8.429/92, art. 13.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio pessoal a fim de ser arquivada no serviço de pessoal competente e pena de demissão para o servidor que se recusar a prestar tal informação ou que a prestar falsa.	Disponibilidade de informações pessoais do agente público para o Poder Público e veracidade dos dados.
Lei nº 8.443/92,	Dever do servidor que exerce	Proteção das

Dispositivo	Mandamento Legal	Aspecto da SI
art. 86, inciso IV.	funções específicas de controle externo no TCU de guardar sigilo sobre dados e informações obtidos em decorrência do exercício de suas funções e pertinentes aos assuntos sob sua fiscalização, utilizando-os, exclusivamente, para a elaboração de pareceres e relatórios destinados à chefia imediata.	informações sigilosas acessadas no exercício de cargo, função ou emprego público.
Lei Complementar nº 75/93, art. 8º incisos II e VIII, §§ 1º e 2º.	Competência do Ministério Público da União para requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta e ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública, bem como a responsabilização pelo uso dessas informações.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.625/93, art. 26, inciso I, alínea b e inciso II.	Competência do Ministério Público de requisitar informações, exames periciais e documentos de autoridades federais, estaduais e municipais, bem como dos órgãos e entidades da administração direta, indireta ou fundacional, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios e requisitar informações e documentos a entidades privadas, para instruir procedimentos ou processo em que oficie.	Proteção da disponibilidade e sigilo das informações constantes nos registros públicos.
Lei nº 8.906/94, art. 7º, inciso XIX.	Direito do advogado de resguardar o sigilo profissional.	Proteção da privacidade do cliente do advogado.
Lei nº 9.100/95, art. 67, incisos VII e VIII.	Constitui crime de fraude eleitoral nas eleições municipais as condutas de:	Proteção da integridade e autenticidade dos sistemas informatizados e

Dispositivo	Mandamento Legal	Aspecto da SI
	(a) obter ou tentar obter, indevidamente, acesso a sistema de tratamento automático de dados utilizado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos; e (b) tentar desenvolver ou introduzir comando, instrução ou programa de computador, capaz de destruir, apagar, eliminar, alterar, gravar ou transmitir dado, instrução ou programa ou provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados utilizado pelo serviço eleitoral.	das informações neles armazenadas.
Lei nº 9.279/96, art. 195, inciso XI.	Constitui crime de concorrência desleal divulgar, explorar ou utilizar, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato.	Proteção da privacidade das pessoas jurídicas, relacionado ao sigilo de suas informações.
Lei nº 9.296/96, art. 10.	Pena de dois a quatro anos, e multa por crime de interceptação de comunicações telefônicas, de informática ou telemática, ou quebra de segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.	Sigilo dos dados e das comunicações privadas.
Lei nº 9.472/97, art. 3º, inciso V.	O usuário de serviços de telecomunicações tem direito à inviolabilidade e ao segredo de sua comunicação, salvo	Sigilo das comunicações.

Dispositivo	Mandamento Legal	Aspecto da SI
	nas hipóteses e condições constitucional e legalmente previstas.	
Lei nº 9.472/97, art. 3º, inciso VI.	O usuário de serviços de telecomunicações tem direito à não divulgação, caso o requeira, de seu código de acesso.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.472/97, art. 3º, inciso IX.	O usuário de serviços de telecomunicações tem direito ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço.	Proteção de informações pessoais de caráter sigiloso.
Lei nº 9.504/97, art. 72.	Pena de 5 a 10 anos pelas condutas de obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou a contagem de votos; desenvolver ou introduzir comando, instrução, ou programa de computador capaz de provocar qualquer outro resultado diverso do esperado em sistema de tratamento automático de dados usados pelo serviço eleitoral; causar, propositadamente, dano físico ao equipamento usado na votação ou na totalização de votos ou a suas partes.	Proteção da integridade das informações de caráter eleitoral e dos equipamentos.
Lei nº 9.605/98, art. 62.	Pena de 1 a 3 anos e multa pela conduta de destruir, inutilizar ou deteriorar arquivo, registro, museu, biblioteca, pinacoteca, instalação científica ou similar protegido por lei, ato administrativo ou decisão judicial.	Disponibilidade e integridade de dados e informações.
Lei nº 10.683/03, art. 6º.	Prevê a competência do GSIPR de coordenar a atividade de segurança da informação.	Todos os aspectos da segurança da informação.

Dispositivo	Mandamento Legal	Aspecto da SI
Lei n.º 10.703/03, arts. 1º , 2º e 3º, de 18 de julho de 2003.	Incumbe aos prestadores de serviços de telecomunicações na modalidade pré-paga, em operação no território nacional, manter cadastro atualizado de usuários. Os dados constantes do cadastro, salvo motivo justificado, deverão ser imediatamente disponibilizados pelos prestadores de serviços para atender solicitação da autoridade judicial, sob pena de multa de até R$ 10.000,00 (dez mil reais) por infração cometida.	Disponibilidade de dados cadastrais para fins de investigação criminal e sigilo nas demais hipóteses.
Decreto nº 4.801/03, art. 1º, inciso X.	Atribuição da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de formular políticas públicas e diretrizes, aprovar, promover a articulação e acompanhar a implementação dos programas e ações estabelecidos no âmbito da segurança da informação.	Todos os aspectos da segurança da informação.
Decreto nº 5.483/05, arts. 3º e 11.	Dever do agente público de apresentar anualmente sua declaração de bens e valores que integram o seu patrimônio e dever de sigilo por parte da Administração Pública dessas informações.	Disponibilidade de informações pessoais do agente público para o Poder Público e dever de sigilo por parte da Controladoria-Geral da União.
Decreto nº 5.687/06, arts.10 e 13 do Anexo.	Convenção das Nações Unidas contra a Corrupção aprovada pelo Congresso Nacional e promulgada pelo Decreto nº 5.687/06, segundo a qual, cada Estado signatário deve esforçar-se para implementar, entre outras, as seguintes medidas: art. 10: a) instaurar procedimentos ou regulamentações que	Disponibilidade das informações públicas ou administrativas e sigilo das informações pessoais constantes nos registros públicos.

Dispositivo	Mandamento Legal	Aspecto da SI
	permitam ao público em geral obter informação sobre a organização, o funcionamento e os processos de adoção de decisões de sua administração pública, com o devido respeito à proteção da intimidade e dos documentos pessoais; b) simplificar procedimentos administrativos a fim de facilitar o acesso do público às informações; c) dar publicidade às informações; - art. 13: a) aumentar a transparência e promover a contribuição da cidadania aos processos de adoção de decisões; b) garantir o acesso eficaz do público à informação.	
Decreto nº 6.029/07, inciso II do art. 1º.	O Sistema de Gestão da Ética do Poder Executivo Federal tem como um de seus objetivos contribuir para a implementação de políticas públicas tendo a transparência e o acesso à informação como instrumentos fundamentais para o exercício de gestão da ética pública.	Disponibilidade das informações constantes nos registros públicos
Decreto nº 6.029/07, art. 10.	Nos trabalhos das Comissões de Ética deverão ser observados os princípios da proteção à honra e à imagem do investigado, bem como proteção à identidade do denunciante, que deverá ser mantida sob reserva se este o desejar.	Sigilo da identidade do denunciante e sigilo do processo para proteção da honra e da imagem do investigado antes da prolação da decisão pela Comissão de Ética.
Decreto nº 6.029/07, art. 13.	Serão classificados como “reservados” os procedimentos de investigação de condutas antiéticas. Concluída a investigação e após a	Sigilo do processo administrativo por infração ética antes da prolação da decisão e publicidade após o término e aplicação das

Dispositivo	Mandamento Legal	Aspecto da SI
	deliberação da Comissão de Ética, o processo deixará de ser “reservado”.	penalidades.
Decreto nº 6.029/07, art. 22.	Comissão de Ética Pública manterá banco de dados de sanções aplicadas para fins de consulta antes de novas nomeações.	Disponibilidade, integridade e autenticidade das informações constantes no banco de dados mantido pela Comissão de Ética Pública.

*Fonte: GSIPR/DSIC (*http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#quadro1*).*

Anexo VI - Legislação específica de caráter Federal

Regulamento	Assunto
Lei nº 7.232, de 29 de outubro de 1984.	Dispõe sobre a Política Nacional de Informática, e dá outras providências.
Lei nº 8.248, de 23 de outubro de 1991	Dispõe sobre a capacitação e competitividade do setor de informática e automação, e dá outras providências.
Lei nº 9.296, de 24 de julho de 1996.	Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal que dispõe sobre a violação do sigilo de dados e das comunicações telefônicas.
Lei nº 9.472, de 16 de julho de 1997	Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais.
Lei nº 9.507, de 12 de novembro de 1997.	Regula o direito de acesso a informações e disciplina o rito processual do habeas data.
Lei nº 9.609, de 19 de fevereiro de 1998.	Dispõe sobre a proteção de propriedade intelectual de programa de computador, sua comercialização no país, e dá outras providências.
Lei nº 9.883, de 07 de dezembro de 1999.	Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências.
Lei nº 8.159/91, de 08 de janeiro de 2001.	Dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências.
Lei Complementar 105, de 10 de janeiro de 2001.	Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências.
Medida Provisória nº 2.200-2, de 24 de agosto de 2001.	Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.
Lei nº 10.973, de 02 de dezembro de 2004.	Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências.
Lei nº 11.111, de 05 de maio de 2005.	Regula o direito à informação e ao acesso aos registros públicos.
Lei nº 11.419, de 19 de dezembro de 2006.	Dispõe sobre a informatização do processo judicial; altera a Lei nº 5.869, de 11 de janeiro de 1973 – Código de Processo Civil; e dá outras providências.
Decreto nº 2.295, 04 de agosto de 1997.	Regulamenta o disposto no art. 24, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Neste caso o processo deverá ser sigiloso, excetuando-se a publicidade das compras governamentais.
Decreto nº 2.556, de 20 de abril de 1998.	Regulamenta o registro previsto no art. 3º da Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua

Regulamento	Assunto
	comercialização no país, e dá outras providências.
Decreto nº 3.294, de 15 de dezembro de 1999.	Institui Programa Sociedade da Informação, com objetivo de viabilizar a nova geração da Internet e suas aplicações em benefício da sociedade brasileira.
Decreto nº 3.505, de 13 de junho de 2000.	Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
Decreto de 18 de outubro de 2000.	Cria, no âmbito do Conselho de Governo, o Comitê Executivo do Governo Eletrônico, e dá outras providências.
Decreto nº 3.714, 03 de janeiro de 2001.	Dispõe sobre a remessa por meio eletrônico de documentos a que se refere o art. 57-A do Decreto no 2.954, de 29 de janeiro de 1999, e dá outras providências.
Decreto nº 3.996, de 31 de outubro de 2001.	Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal.
Decreto nº 4.073, de 03 de janeiro de 2002.	Regulamenta a Lei nº 8.159, de 08 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.
Decreto nº 4.376, de 13 de setembro de 2002.	Dispõe sobre a organização e o funcionamento do Sistema Brasileiro de Inteligência, e dá outras providências.
Decreto nº 4.522, 17 de dezembro de 2002.	Dispõe sobre o Sistema de Geração e Tramitação de Documentos Oficiais - SIDOF, e dá outras providências.
Decreto nº 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 Pública Federal, e dá outras providências.
Decreto nº 4.689, de 07 de maio de 2003.	Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão do Instituto Nacional de Tecnologia da Informação – ITI, e dá outras providências.
Decreto nº 4.829, de 03 de setembro de 2003.	Dispõe sobre a criação do Comitê Gestor da Internet no Brasil – CGIbr, sobre o modelo de governança da Internet no Brasil, e dá outras providências.
Decreto de 29 de outubro de 2003.	Institui Comitês Técnicos do Comitê Executivo do Governo Eletrônico e dá outras providências.
Decreto nº 5.301, de 09 de dezembro de 2004.	Institui a Comissão de Averiguação e Análise de Informações Sigilosas, dispõe sobre suas atribuições e regula seu funcionamento.
Decreto nº 5.450, de 31 de maio de 2005.	Regulamenta o pregão, na forma eletrônica, para aquisição de bens e serviços comuns, e dá outras providências.
Decreto nº 5.563, de 11 de outubro de 2005.	Regulamenta a Lei nº 10.973, de 02/12/04, que dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo, e dá outras providências.

Regulamento	Assunto
Decreto nº 5.584, de 18 de novembro de 2005.	Dispõe sobre o recolhimento ao Arquivo Nacional dos documentos arquivísticos públicos produzidos e recebidos pelos extintos Conselho de Segurança Nacional - CSN, Comissão Geral de Investigações - CGI e Serviço Nacional de Informações - SNI, que estejam sob a custódia da Agência Brasileira de Inteligência - ABIN.
Decreto nº 5.772, de 08 de maio de 2006, art. 8º.	Institui na estrutura regimental do Gabinete de Segurança Institucional da Presidência da República o Departamento de Segurança da Informação e Comunicações com diversas atribuições na área de segurança da informação e comunicações.
Decreto nº 6.605, de 14 de outubro de 2008.	Dispõe sobre o Comitê Gestor da Infra-Estrutura de Chaves Públicas Brasileira - CG ICP-Brasil, sua Secretaria-Executiva e sua Comissão Técnica Executiva - COTEC.
Instrução Normativa nº 1 do GSI, de 13 de junho de 2008.	Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Resolução nº 58 do INPI, de 14 de julho de 1998.	Estabelece normas e procedimentos relativos ao registro de programas de computador.
Resolução nº 59 do INPI, de 14 de julho de 1998.	Estabelece os valores das retribuições pelos serviços de registro de programas de computador.
Resolução nº 338 do STF, de 11 de abril de 2007.	Dispõe sobre classificação, acesso, manuseio, reprodução, transporte e guarda de documentos e processos de natureza sigilosa no âmbito do STF.
Resolução nº 140 do TST, de 13 de setembro de 2007.	Regulamenta, no âmbito da Justiça do Trabalho, a Lei n° 11.419, de 19 de dezembro de 2006, que dispõe sobre a informatização do processo judicial.
Resolução nº 22.718/08 do TSE, arts. 18 e 19.	Regula a propaganda eleitoral na internet em campanha nas eleições de 2008.

*Fonte: GSIPR/DSIC (*http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#quadro2*).*

Anexo VII - Legislação específica de caráter Estadual/Distrital

Regulamento	Assunto
Lei Distrital nº 3.437, de 09 setembro de 2004.	Dispõe sobre o cadastro dos usuários das empresas ou instituições que locam ou cedem gratuitamente computadores e máquinas para acesso à Internet, no âmbito do Distrito Federal, conhecidas também como “cyber-cafés”.
Lei Estadual de São Paulo nº 12.228, de 11 de janeiro de 2006.	Dispõe sobre os estabelecimentos comerciais que colocam a disposição, mediante locação, computadores e máquinas para acesso à Internet e dá outras providências.
Lei Estadual do Rio Grande do Sul nº 12.698, de 04 de maio de 2007.	Dispõe sobre a proteção da saúde dos consumidores nos estabelecimentos comerciais que ofertam a locação e o respectivo acesso a jogos de computador em rede local, conhecidos como "LAN house" - "Local Área Network" -, e seus correlatos, e dá outras providências, dentre as quais a exigência de cadastramento dos menores de 18 anos que frequentam o local.
Lei Estadual de São Paulo nº 12.906, de 14 de abril de 2008.	Estabelece normas suplementares de direito penitenciário e regula a vigilância eletrônica, e dá outras providências.
Decreto Estadual do Paraná nº 5.111, de 19 de julho de 2005.	Estabelece diretrizes para o licenciamento de programas de computador de titularidade de entidades da Administração Estadual na Licença Pública Geral da Administração Pública – LPG-AP, e dá outras providências.

*Fonte: GSIPR/DSIC (*http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#quadro3*).*

Anexo VIII - Legislação específica de caráter Municipal

Regulamento	Assunto
Lei Municipal de Farroupilha-RS nº 3.087, de 29 de dezembro de 2005.	Dispõe sobre o funcionamento das casas de jogos por computador conhecidos como Lan Houses, e dá outras providências, dentre as quais a exigência de cadastramento dos menores de 18 anos que frequentam o local.

*Fonte: GSIPR/DSIC (*http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#quadro4*).*

Anexo IX - Normas técnicas

Regulamento	Assunto
ISO/IEC TR 13335-3:1998.	Esta norma fornece técnicas para a gestão de segurança na área de tecnologia da informação. Baseada na norma ISO/IEC 13335-1 e TR ISO/IEC 13335-2. As orientações são projetadas para auxiliar o incremento da segurança na TI.
ISO/IEC GUIDE 51:1999.	Esta norma fornece aos elaboradores de normas recomendações para a inclusão dos aspectos de segurança nestes documentos. É aplicável a qualquer aspecto de segurança relacionado a pessoas, propriedades, ao ambiente, ou a uma combinação de um ou mais destes (por exemplo, somente pessoas; pessoas e propriedades; pessoas, propriedades e o ambiente).
ISO/IEC GUIDE 73:2002.	Esta norma fornece definições genéricas de termos de gestão de riscos para a elaboração de normas. Seu propósito é ser um documento genérico de alto nível voltado para a preparação ou revisão de normas que incluam aspectos de gestão de riscos.
ABNT NBR ISO IEC 17799: 2005.	Esta norma é equivalente à ISO/IEC 17799:2005. Consiste em um guia prático que estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Os objetivos de controle e os controles definidos nesta norma têm como finalidade atender aos requisitos identificados na análise/avaliação de riscos.
ABNT NBR ISO/IEC 27001:2005.	Esta norma é usada para fins de certificação e substitui a norma Britânica BS 7799-2:2002. Aplicável a qualquer organização, independente do seu ramo de atuação, define requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação.

*Fonte: GSIPR/DSIC (*http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm#quadro5*).*