IX SEGeT 2012
SIMPÓSIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA
Tema: Gestão, Inovação e Tecnologia para a Sustentabilidade

Processo de Elaboração do Plano de Segurança da Informação do Instituto Federal de Educação, Ciencia e Tecnologia Catarinense - Ifc

Clovis Cristiano Brignoli
ccbrignoli@ifc-riodosul.edu.br
Unidavi-IFC Rio Sul

Fabio Alexandrini
fabalexandrini@yahoo.com.br
Unidavi-IFC Rio Sul

Tiago Boechel
tboechel@gmail.com
IFC Rio do Sul

Thiago Souza Araujo
prof.araujo@unidavi.edu.br
Unidavi-USJ

José Ernesto De Faveri
faveri@unidavi.edu.br
Unidavi

Resumo: Os Institutos Federais de Educação, Ciência e Tecnologia são instituições que disponibilizam a população a oferta de educação superior, básica e profissional, pluricurriculares e multicampi, especializados em educação profissional e tecnológica em diferentes modalidades de ensino, e baseado em conhecimentos técnicos e tecnológicos às suas práticas pedagógicas, compondo assim a Rede de Educação Profissional, Científica e Tecnológica do Ministério da Educação, e criada no final de 2008. Frente a estas modificações estabelecidas pelo Governo Federal junto à educação de todo o país, percebe-se que em praticamente todas as áreas dos novos institutos existiram mudanças significativas durante esta mudança. A pesquisa realizada neste artigo possui como principal objetivo, a tentativa de proporcionar uma base para que o Instituto Federal de Educação, Ciência e Tecnologia Catarinense - Campus Rio do Sul, em meio a sua mudança de Autarquia Federal, quando Agrotécnica, para Campi do Instituto Federal, para a criação e o estabelecimento de regras, normas e procedimentos, para a área de Tecnologia da Informação, necessitando ser adotado neste novo modelo. Para tanto, vem sendo constantemente realizados estudos para a criação de um Comitê Gestor de Tecnologia da Informação para o auxilio, implantação e implementação de um Plano de Segurança da informação nos campis do instituto.

Palavras Chave: Plano Diretor TI - Institutos Federais - Adm.Sist. Informação - Segurança da Informa -

INTRODUÇÃO

Com o intuito de promover um vinculo com a valorização da educação e das instituições publicas, fundamental para a construção de uma nação soberana e democrática, pressupondo o combate as desigualdades estruturais, em 29 de dezembro de 2008, pela Lei n°.11.892, foram criados trinta e oito Institutos Federais de Educação, Ciência e Tecnologia em todo o Brasil.

Dentre estes, foi criado o Instituto Federal de Educação, Ciência e Tecnologia Catarinense - IFC, uma integração entre as Escolas Agrotécnicas Federais de Concórdia, Rio do Sul, e Sombrio e os Colégios Agrícolas de Araquari e Camboriú, e com uma Reitoria em Blumenau, todos estes distribuídos pelo estado de Santa Catarina.

Oferecendo educação em todos os níveis, desde a formação inicial e continuada até a pós-graduação, tenta buscar o atendimento de demandas regionais das localizações dos Campi, tendo como meta principal a interferência positiva na transformação da realidade econômica e social local, e a contribuição no desenvolvimento de arranjos produtivos locais e regionais.

Com sua origem intimamente ligada a problemas econômicos e sociais, percebidos desde a década de 1970 no Alto Vale Catarinense, o Instituto Federal Catarinense - Campus Rio do Sul, antiga Escola Agrotécnica Federal de Rio do Sul, que possuía a principio, seu foco voltado diretamente a cursos nas áreas agrícolas, com a crescente expansão do ensino e as novas dimensões da educação no país, primando sempre pela educação pública, gratuita e de qualidade, oportunizou novos focos de educação, dentre os quais contempla áreas como a da informática, eletroeletrônica, agrimensura, matemática, física, agricultura, agroecologia, florestas e zootecnias.

Tendo em vista o atendimento de uma grande demanda de alunos e colaboradores, possuem em suas dependências físicas, laboratórios, salas de aula, auditórios, bibliotecas e estruturas funcionais, favorecendo a realização de atividades voltadas ao ensino, pesquisa, desenvolvimento e extensão.

Em sua grande maioria, as estruturas são informatizadas, e disponibilizam estrutura de rede intranet e internet para toda a comunidade escolar e em todos os *Câmpus* do Instituto. Para que a implementação de todas as estratégias a serem utilizadas sejam iguais em todo o Instituto Federal Catarinense, faz-se necessário, a execução de normatizações relativas a toda a área de Tecnologia da Informação, obedecendo aos padrões estabelecidos pelo Governo Federal.

Na figura 01, pode-se perceber claramente a localização da Reitoria do Instituto Federal Catarinense, em relação aos *Câmpus* do Instituto em todo o estado, verificando que existem alguns que possuem uma distancia geográfica grande.

Reitoria (Blumenau)		
1-	IFC - Câmpus de Araquari	84,4 Km
2-	IFC - Câmpus de Blumenau	12,9 Km
3-	IFC - Câmpus de Camboriú	73,7 Km
4-	IFC - Câmpus de Concordia	398 Km
5-	IFC - Câmpus de Ibirama	78,9 Km
6-	IFC - Câmpus de Luzerna	324 Km
7-	IFC - Câmpus de Rio do Sul	101 Km
8-	IFC - Câmpus de São Francisco do Sul	111 Km
9-	IFC - Câmpus de Sombrio	350 Km
10-	IFC - Câmpus de Videira	312 Km

Distancia Aproximada da Reitoria em relação aos Câmpus

Fonte: Acervo do Autor

Figura 01: Mapa de Santa Catarina, com a localização dos Câmpus e Reitoria do Instituto Federal Catarinense.

OBJETIVOS E JUSTIFICATIVA

Este estudo possui como objetivo principal, proporcionar uma base para que o Instituto Federal de Educação, Ciência e Tecnologia Catarinense - *Câmpus* Rio do Sul, em meio a sua mudança de Autarquia Federal, quando Agrotécnica, para *Câmpus* do Instituto Federal, consiga estabelecer regras de normas e procedimentos, no tocante a segurança da informação, na área de Tecnologia da Informação, a serem adotados neste novo modelo.

Tendo em vista este novo modelo adotado pelo Governo Federal, onde antes todos os problemas encontrados eram solucionados diretamente pela alta administração da escola, agora as decisões não são mais tomadas diretamente pelos *Câmpus*, mas sim pela Reitoria, que possui como premissa a administração do cotidiano de todos os *Câmpus*do Instituto, bem como o planejamento de seu futuro, atendendo os anseios da comunidade interna e externa ao Instituto.

Pensando nisso, foi criado um Comitê Gestor de Tecnologia da Informação – CGTI, órgão colegiado, de natureza deliberativa e de caráter permanente, criado pelo Reitor do IFC e em conformidade com as orientações da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG e pelo Sistema de Administração e Recursos de Informação e Informática - SISP.

Este comitê torna-se responsável pelo alinhamento dos investimentos de Tecnologia da Informação com os objetivos institucionais, definindo qual a prioridade dos projetos de Tecnologia da Informação, possuindo como finalidade a tomada de decisões relacionadas à Tecnologia da Informação no âmbito do Instituto Federal Catarinense.

Uma das metas deste comitê são o estabelecimento e a implantação de um Sistema de Gestão de Segurança da Informação - SGSI, representando um avanço dentro do instituto no tocante a segurança das informações, percebendo-se que cada vez mais, a existência de uma sensibilidade sobre a necessidade da agregação da segurança aos negócios, independente do ramo de atividade exercida pela organização.

Possibilitando a integração de metodologias e de boas práticas que podem ser aplicadas em toda a organização, oSistema de Gestão de Segurança da Informação - SGSI integra e alinha os processos e procedimentos das áreas de negócios e de Tecnologia da Informação, e após sua implementação deve ser constantemente atualizada, revista, monitorada, atualizada, ajustada e acompanhada, estabelecendo metas e indicadores, mantendo-as alinhadas aos processos estratégicos da organização e da segurança da informação.

REDES DE COMUNICAÇÃO

A Comunicação é a forma como as pessoas se relacionam entre si, dividindo e trocando experiências, idéias, sentimentos, informações, modificando mutuamente a sociedade onde estão inseridas. Sem a comunicação, cada um de nós seria um mundo isolado (BORDENAVE, 2002).

Para Bordenave (2002), comunicar é tornar comum, podendo ser um ato de mão única, como transmitir, onde um emissor transmite uma informação a um receptor, ou de mão dupla, como compartilhar, onde os emissores e receptores constroem o saber, a informação, e depois a transmitem. A comunicação é a representação de uma realidade e serve para partilhar emoções, sentimentos e informações.

Segundo Bordenave (2002), quem comunica é a fonte, e de outro lado está o receptor, sendo que, o que é comunicado é a mensagem. Pode ser vista, ouvida, tocada em forma de mensagem que podem ser palavras, gestos, olhares, movimentos do corpo. As formas como as idéias são representadas são chamadas de signos, que em conjunto, formam os códigos, que podem ser a língua, os códigos, ou os sinais.

> “Os meios são usados pelos interlocutores para transmitir sua mensagem. O locutor usa sua voz, o roteiro, a emissora.” (BORDENAVE, 2002).
> Antes do surgimento dos meios tecnológicos de transmissão de informação (TV, rádio, internet etc.), os meios de comunicação utilizados eram físicos, como os rios, navios e estradas.

A comunicação está contida no nosso ambiente social. Em uma conversa, em um gesto qualquer, em um sinal, em um espetáculo ou em um diálogo entre surdos-mudos, só para citar alguns exemplos. É impossível dissociar de nossa vida, nossas necessidades, da comunicação.

Estudos revelam que os meios de comunicação exercem influências positivas e negativas na vida das pessoas, como jornais que podem ajudar na tomada de decisões importantes, propiciar o estabelecimento de contatos sociais e dar status (atributo intangível).

Os homens encontraram uma forma de associar um som ou objeto a um gesto ou ação. Assim nasceu o signo, que é qualquer coisa que faça referência a outra coisa, dando-lhe uma significação. Os signos podem ser representados por símbolos, objetos físicos que dão significação moral, como a bandeira e hino nacional, mulher cega segurando uma balança ou as alianças de um casal, e sinais, que são indícios que possibilitam conhecer, reconhecer ou prever algo, como sinais de trânsito, sinais ortográficos, sinais de luzes nos aeroportos e nas traseiras dos carros.

REDES DE COMPUTADORES

O inicio das redes de comunicação foi em meados do século XIX, com o telegrafo, e com ligações de usuários com sistemas de linhas telefônicas ponto a ponto realizadas por

Graham Bell. Partindo daí, as redes de comunicação só tenderam a ampliar suas fronteiras, com redes de comunicações convencionais, fixas e móveis, redes de TV a cabo e sistemas de transmissão de energia elétrica utilizados para a transmissão de informação.

Os primeiros computadores conhecidos começaram a ser desenvolvido, em meados da década de 1930, juntamente com a ideia de interligação entre eles, dispersos geograficamente o que era denominado como teleprocessamento, termo reservado até então, pela IBM (*International Business Machines*).

Uma rede de computadores é formada por um ou mais computadores conectados um ao outro por um meio de transmissão, sendo capaz de trocar informações e compartilhar recursos (TANENBAUM, 2003).

O modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas redes de computadores, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados (TANENBAUM 2003).

Segundo Dantas (2002), uma rede de computadores pode ser definida segundo seu tamanho ou sua área de abrangência física. Quando sua abrangência é de poucos quilômetros é conhecida como LAN (Local Area Network) ao passo que em casos com uma maior abrangência, como redes metropolitanas abrangendo a região metropolitana de uma cidade é conhecida como MAN (MetropolitanArea Network). Uma rede geograficamente distribuída que pode englobar até o mundo inteiro é conhecida como WAN (WideArea Network)

Para Peterson e Davie (2004), tanto para uma rede de pequena abrangência quanto para uma rede mundial, a montagem dos hardwares dela é feito através de duas classes de blocos, os nós e os enlaces, onde os nós ou nodos geralmente são computadores de uso geral, de uso pessoal ou estações de trabalho, enquanto que os enlaces são os meios físicos utilizados para a realização das conexões entre os nós.

Conforme Tanenbaum (1997), uma das mais primitivas topologias é o barramento, ligando os nós em series através de um único cabo (barramento), utilizada na comunicação com caminhos bidirecionais, que quando um dos nós deseja transmitir, este verifica se o barramento está ocupado e se não estiver é iniciada então a transmissão, caracterizando-se pelo fato de que se existir um rompimento de algum ponto deste barramento, comprometerá então toda a rede.

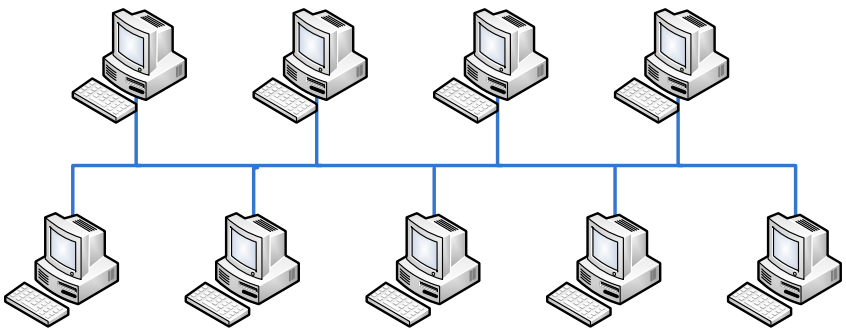

Figura 02: Topologia em Barramento
Fonte: Adaptado de Tanenbaum (1997)

Para Tanenbaum (1997), na topologia anel os nós são conectados em series, constituindo um sistema fechado, onde a transmissão dos dados é unidirecional e passa por cada nó até chegar ao seu destino, ocorrendo retransmissões sucessivas até que o nó de destino retire sua mensagem que foi enviada pelo nó de origem. A distorção e a atenuação do sinal, comparando-se com a topologia de barramento é menos devido à repetição do sinal por cada nó.

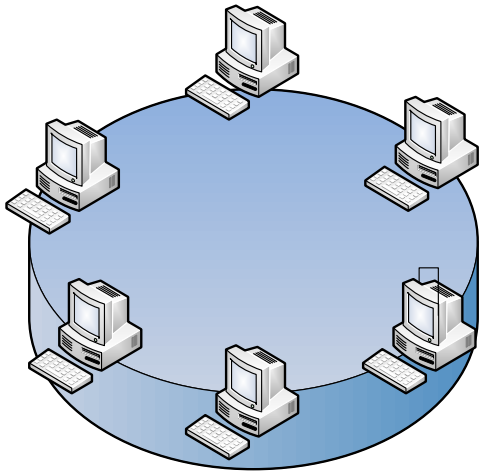

Figura 03: Topologia em Anel
Fonte: Adaptado de Tanenbaum (1997)

Ainda conforme Tanenbaum (1997), na topologia estrela os nós são interconectados por cabos interligados em uma só central, que ao contrário das topologias em barramento ou em anel, quando ao acaso ocorrer um rompimento entre algum enlace, a rede continuará operando normalmente, apenas com a parada de alguns equipamentos.

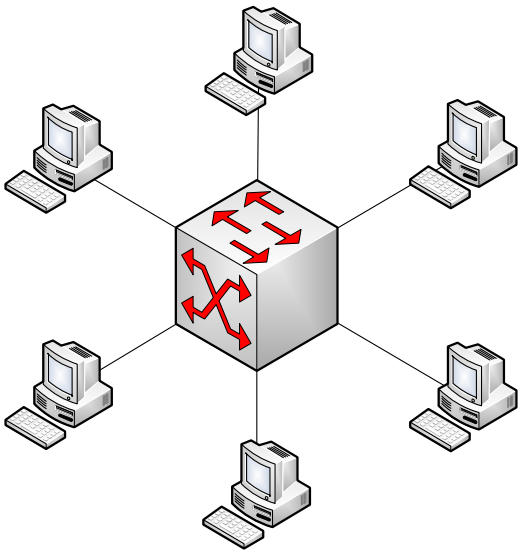

Figura 04: Topologia em Estrela
Fonte: Adaptado de Tanenbaum (1997)

Para Peterson e Davie (2004), a garantia de requisitos como a conectividade, o compartilhamento de recursos e o suporte para serviços comuns sejam contemplados em um projeto de rede, este deverá ser implementado e orientado, através do conceito de um conjunto de camadas e de protocolos, conhecidos como arquitetura de rede.

Dantas (2002) define que para que duas estações de trabalho se comuniquem, é necessário que exista uma determinação de um conjunto de regras de comunicação e de tratamento para os erros, devendo-se definir o formato adequado dos dados (sintaxe) e o

controle das informações, coordenando e tratando os erros (semântica), adequando os tempos de transferência e de sequencias das mensagens (temporização) entre as estações de trabalho, comumente conhecido como protocolo.

Para Kurose e Ross (2006), um protocolo define a ordem e o formato das mensagens que serão trocadas, define também as ações a serem realizadas na transmissão ou no recebimento de uma mensagem ou outro evento.

Kurose e Ross (2006) defendem que a forma encontrada para o controle e a organização dos protocolos da rede é a implementação de camadas (Interconexão de Sistemas Abertos - OSI e Protocolo de Controle de Transmissão/ Protocolo de Internet - TCP/IP), onde cada uma executa ações de sua competência e repassando informações para as camadas superiores sucessivamente, chegando a ultima camada e modularizando o processo.

7	Aplicação		Aplicação
6	Apresentação		
5	Sessão		
4	Transporte		Transporte
3	Rede		Internet
2	Dados		Interface com a rede
1	Física		

Comparação entre os modelos OSI e TCP/IP

Fonte: Adaptado de Tanenbaum (1997)

Tornou-se então, um fator comum entre os fabricantes de computadores, dissipando-se entre estes como o caminho a ser trilhado para que fosse obtido um maior valor computacional agregado, compreendendo que as redes eram a direção apropriada, interligando computadores com arquiteturas distintas de rede.

As redes de comunicação são os ambientes geograficamente distribuídos, responsáveis pela transmissão transparente da voz, imagem, vídeo e dados (numéricos e textos). Podemos dizer que as redes de comunicação se preocupam com a comutação dos dados sem a preocupação do conteúdo dos dados (DANTAS, 2010).

Em uma rede de comunicação comutada, existe a ligação de inúmeras estações conectadas, através de uma nuvem de ligação entre os ambientes de redes de computadores, composta por módulos de comutação (nodos de comutação), interligados por enlaces de transmissão. As comutações podem ser efetuadas de forma distinta, dependendo dos softwares utilizados, e os mecanismos empregados nos pacotes de comutação variam de acordo com as taxas de transmissões, onde podemos encontrar a comutação por circuitos ou por pacotes.

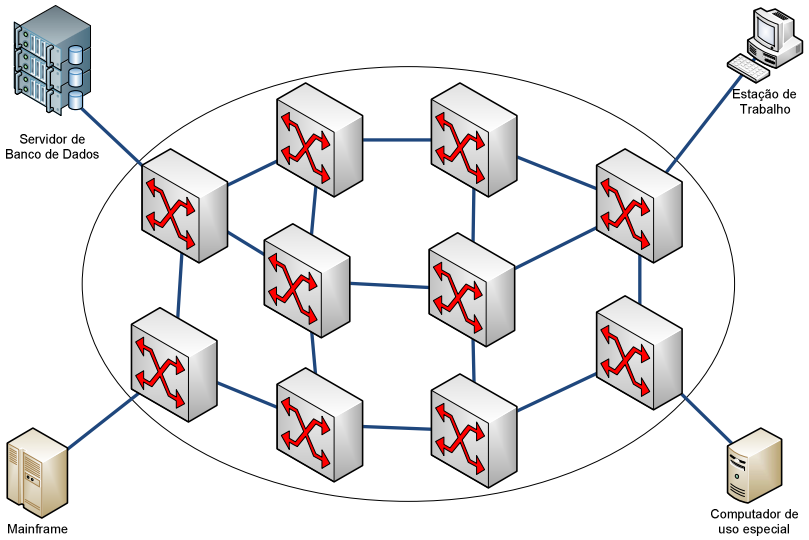

Figura 05: Exemplo de uma rede de Comunicação Comutada
Fonte: Adaptado de Dantas (2010).

Pode-se afirmar que, a interligação local de computadores, conhecido como agregados computacionais ou clusters, que pode ser traduzida como uma evolução de uma simples interconexão física de computadores para uma forma distribuída de operação.

Para Dantas (2010), a rede não deve apenas nos permitir ligar computadores, mas possuirmos garantias de que as aplicações de diferentes fornecedores devem interoperar de uma forma única, transparente e com bom desempenho.

Recentemente, os paradigmas de clusters computacionais ganham novas dimensões das redes geograficamente distribuídas, desenvolvidos sob os paradigmas de grade (*grid*) e nuvem computacional (*cloud computing*).

SEGURANÇA DA INFORMAÇÃO

Os avanços nas telecomunicações e nos sistemas de informação ampliaram as vulnerabilidades, quando grandes quantidades de dados são armazenadas de forma eletrônica, sofrem muito mais tipos de ameaças, do que quando estão em armazenadas de uma forma manual.

Conforme Laudon e Laudon (2004), os sistemas de informação, nas mais diferentes localidades, podem ser interconectados por meio de redes de telecomunicações, potencializando desta forma, o acesso não autorizado, os abusos ou fraudes, não limitando apenas um único local, mas podendo ocorrer em qualquer ponto de acesso à rede.

Além disso, para Laudon e Laudon (2004), arranjos complexos e diversos de hardware, software, pessoais e organizacionais são exigidos para redes de telecomunicação, criando novas áreas e oportunidades para invasão e manipulação, como redes sem fio, que utilizam tecnologias baseadas em rádio, sendo ainda mais vulnerável a invasões, pois são de fácil varredura de faixas de radiofreqüência.

A Internet, por exemplo, apresenta problemas especiais, pois foi projetada para ser acessada facilmente, e por pessoas com sistemas de informações diferentes. Redes de telecomunicação são vulneráveis a falhas naturais de hardware e software, e ao uso indevido por pessoal não autorizado, sendo possível, por exemplo, grampear linhas de telecomunicação e interceptar dados ilegalmente.

O avanço da tecnologia trouxe benefícios incalculáveis para as organizações, mas com esses benefícios vieram também problemas sérios para serem solucionados pela equipe de

Tecnologia da Informação. Agora as empresas têm seus computadores ligados em redes internas e externas, seus dados trafegam por vários lugares, trazendo preocupação com a segurança da rede. A proteção dos sistemas em rede pode ser algo bastante complexo (TURBAN, 2004).

Existem centenas de pontos nos sistemas de informação de uma organização sujeitos a ameaças (TURBAN, 2004). Para tanto, a equipe de gerenciamento de Tecnologia da Informação deve estar constantemente atualizada quanto às vulnerabilidades e sistemas de segurança necessários para se mantiver a rede protegida. A computação em rede é uma tendência nas empresas, surgindo então a necessidade de se planejar as metas de segurança da informação.

Segundo Turbanet al. (2004), os controles de proteção são divididos em duas categorias, Controles Gerais, implantados para proteger os sistemas, independentemente do aplicativo específico, dividindo em controles físicos, controles de acesso, controles de segurança de dados, controles de comunicação (redes) e controles administrativos, não protegendo o conteúdo de cada aplicativo específico, e os Controles de Aplicativos, relatando que os mesmos procuram proteger as instalações de computação e prover segurança para hardware, software, dados e redes.

Frequentemente são estabelecidos controles dentro dos aplicativos, ou seja, fazem parte do software, e normalmente são escritos sob forma de regras de validação, podendo ser classificados em categorias de controles de entrada, impedindo a alteração ou a perda de dados, os controles de processamento, garantindo que os dados sejam completamente processados, sendo válidos e precisos e para que os programas sejam executados corretamente, e os controles de saídas, garantindo que os resultados do processamento sejam precisos, válidos, completos e consistentes.

DESENVOLVIMENTO DO TRABALHO

A informação é um ativo que possui grande valor para as organizações, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que garantam a segurança da informação deve ser prioridade constante da organização, reduzindo os riscos de falhas, os danos e os prejuízos que possam comprometer a imagem e os objetivos da instituição.

A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em mídias de áudio e de vídeo, entre outras.

Um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coleta (ou recupera), processa, armazena e distribui informações destinadas a apoiar a tomada de decisões, a coordenação e o controle de uma organização, além de dar suporte à tomada de decisões, à coordenação e ao controle, esses sistemas também auxiliam os gerentes e trabalhadores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

Em grandes e complexas organizações, a proteção da informação não é uma tarefa comum. A Política de Segurança da Informação adotada por uma instituição depende da combinação de diversos elementos, entre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de diretores, funcionários e colaboradores.

Durante o ano de 2011, foram realizadas na Reitoria do Instituto Federal de Educação, Ciência e Tecnologia Catarinense, reuniões com os responsáveis pela Coordenação de

Tecnologia da Informação de todo o Instituto (*Câmpus* e Reitoria), e através de fóruns de discussão, onde foi identificada uma serie de problemas relativos a todo o Campi do Instituto Federal Catarinense.

As principais demandas encontradas foram à falta de padronização de processos e procedimentos nas áreas de tecnologia da informação, e quanto à unificação de descrição de equipamentos a serem adquiridos e utilizados. Com base nestas reuniões e nos processos já existentes nos diversos órgãos do governo federal, foi iniciada então a instituição de um Comitê Gestor de Tecnologia da Informação - CGTI do Instituto Federal Catarinense.

Com regimento próprio e a atribuição básica de promover o alinhamento dos investimentos em tecnologia da informação com os objetivos do instituto, além da priorização de projetos nesta determinada área, e recomendando, quando necessário, atualizações e ajustes em projetos relativos à Tecnologia da Informação e a comunicação, o Comitê Gestor de Tecnologia da Informação, atualmente ainda em fase embrionária, é constituído pelo Reitor do Instituto Federal Catarinense, responsável pela presidência do Comitê, pelo Diretor de Tecnologia da Informação que ocupa também a função de Secretário Executivo, pelos Pró-reitores de todas as Pró-reitorias, e pelos Diretores Gerais de cada *Câmpus*.

Buscando uma constante melhoria em níveis de tecnologia de informação do Instituto Federal Catarinense, o Comitê Gestor de Tecnologia da Informação, possui como metas principais a analise e a homologação de um Plano Diretor de Tecnologia da Informação - PDTI, observando as diretrizes estabelecidas pelos comitês executivos do Governo Eletrônico, o planejamento anual de aquisições, contratações e serviços de tecnologia da informação, as propostas de estratégias e diretrizes relativas à gestão de recursos de informação e tecnologias associadas, e a criação de grupos de trabalho ou subcomitês para auxiliarem nas decisões do comitê.

SITUACAO ATUAL

Como verificado anteriormente, o Instituto Federal de Educação, Ciência e Tecnologia Catarinense, nasceu de uma junção entre as antigas Escolas Agrotécnicas, vinculadas diretamente ao Ministério da Educação, e dos Colégios Agrícolas, vinculados à Universidade Federal de Santa Catarina.

Cada um deles possuindo, até então, suas peculiaridades e seus vícios, tanto de sua distribuição geográfica quanto de seus participantes. Fazer com que todos os *Câmpus*, agora membros atuais do instituto, juntamente com alguns *Câmpus*novos e recém-inaugurados, torna-se uma tarefa árdua e demorada, mas é uma missão e um desejo intrínseco.

Em discussões realizadas, percebe-se que todos os *Câmpus*existentes, possuem inúmeros equipamentos, seja na área administrativa para uso de servidores técnico administrativos, ou na área pedagógica para uso de professores, além disto, todos os *Câmpus*utilizam-se de laboratórios informatizados para ministrar cursos em áreas afins a tecnologia da informação para os educandos.

Possuem também, servidores ligados diuturnamente, atendendo as necessidades de cada campus e de suas respectivas unidades, sejam servidores de aplicativos, servidores de arquivos, servidores de dados ou servidores de internet, servidores estes que na Reitoria (Blumenau), e nos *Câmpus*de Concordia, Rio do Sul e Sombrio, estão diretamente ligados ao Ponto de Presença da Rede Nacional de Ensino e Pesquisa em Santa Catarina - PoP/SC - RNP, atendendo as necessidades operacionais da rede, a demanda de conectividade e informações a usuários, bem como a coordenação e operação de serviços de internet em Santa Catarina. Todo esse serviço é realizado sem custo para o Instituto Federal Catarinense e, além disto, com propostas de melhoria de sinais para os *Câmpus*já conectados e de novas conexões

a serem realizadas para os novos *Câmpus*e novas unidades.

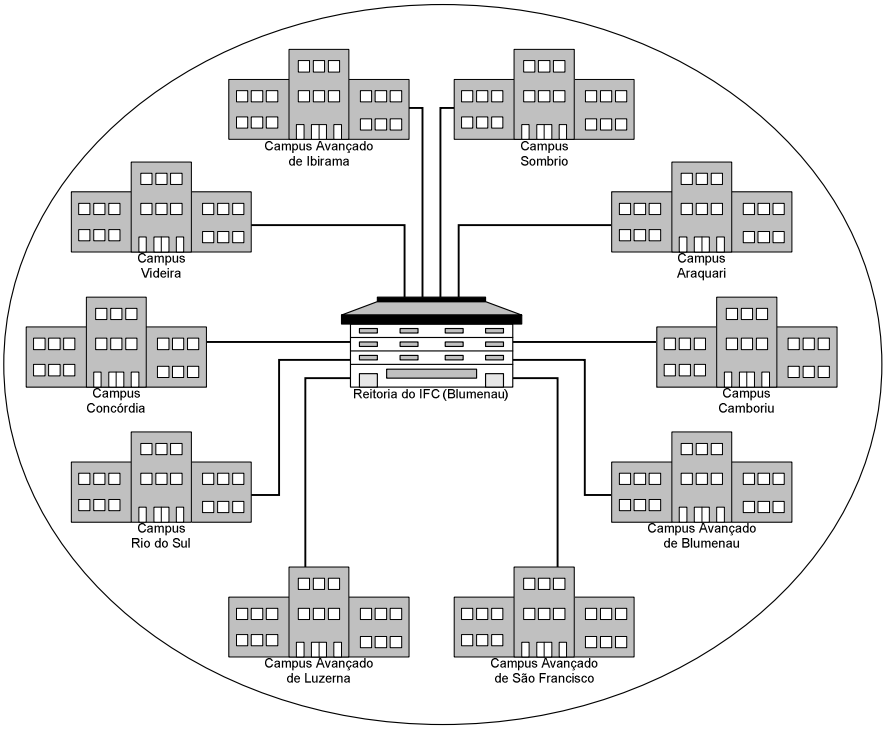

Figura 06: Estrutura atual dos Campi do IFC
Fonte: Acervo do Autor

PLANO DE SEGURANÇA DA INFORMAÇÃO - PROPOSTA

Conforme Laureano e Moraes (2005), os sistemas que administram as informações devem respeitar os seguintes critérios: autenticidade, não repúdio, privacidade e auditoria.

Inicialmente, deve-se possuir a percepção de que a segurança da informação deve abranger três aspectos básicos:

- A confidencialidade, onde somente pessoas devidamente autorizadas pela empresa devem possuir o acesso à informação.

- A Integridade, onde somente poderão ser realizadas alterações, supressões e adições autorizadas pela empresa, devem ser realizadas nas informações.

- A disponibilidade, pois a informação deve estar disponível, apenas para as pessoas autorizadas sempre que necessário ou demandado.

Para que se possam assegurar esses itens, a informação deve ser adequadamente gerenciada e protegida contra qualquer tipo de roubo, fraude, espionagem, perda não intencional, acidentes e outras possíveis ameaças.

A Política de Segurança da Informação deve ser uma declaração formal da organização, acerca de seu compromisso com a proteção das informações de sua propriedade ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, com o propósito de estabelecer diretrizes a serem seguidas, no tocante à adoção de procedimentos e mecanismos relacionados à segurança da informação.

Independentemente do meio ou da forma existente, a informação está presente no trabalho de todos os profissionais, e desta forma, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações, destacando-se, por exemplo, diretores, coordenadores, servidores e terceirizados, devem assumir atitude proativa e engajada no que diz respeito à

proteção das informações, todos os servidores devem compreender as ameaças externas que podem afetar a segurança das informações da organização, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, entre outros, bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.

Todo tipo de acesso à informação do Instituto Federal Catarinense, que não for explicitamente autorizado é proibido.

Informações confidenciais, não devem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.

Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).

As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não protegido.

Somente softwares homologados pelos especialistas do Instituto Federal Catarinense, podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de Tecnologia da Informação do Instituto Federal Catarinense.

As políticas para uso de internet e correios eletrônicos devem ser rigorosamente seguidas, e arquivos de origem desconhecida nunca devem ser abertos ou executados.

Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.

Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação.

A área de Gestão de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos de incidentes relacionados à segurança da informação.

A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Gestor da Segurança da Informação, principalmente, no que diz respeito à identificação dos principais riscos aos quais as informações do Instituto Federal Catarinense estarão expostas e priorização de ações voltadas à mitigação dos riscos apontados, tais como a implantação de novos controles, criação de novas regras e procedimentos ou a reformulação de sistemas.

O escopo da análise ou da avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.

Alguns sistemas (como SIGA ADM, SIGA EDU, Pergamun), ainda que em fase terminal de implantação, implementação e padronização para todo o Instituto, as informações e os serviços utilizados pelos usuários deverão ser de exclusiva propriedade do Instituto Federal Catarinense, não podendo ser interpretados como de uso pessoal.

Conforme as demandas irão aparecendo, e visto a necessidade de outros sistemas integrados que contribuem para a informatização de diversas áreas comuns do instituto e seus *Câmpus*, serão implementadas novas ferramentas padronizadas.

Todos os profissionais e servidores do Instituto Federal Catarinense deverão ter ciência de que, o uso das informações e dos sistemas de informação, podem ser monitorados, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos ou legais.

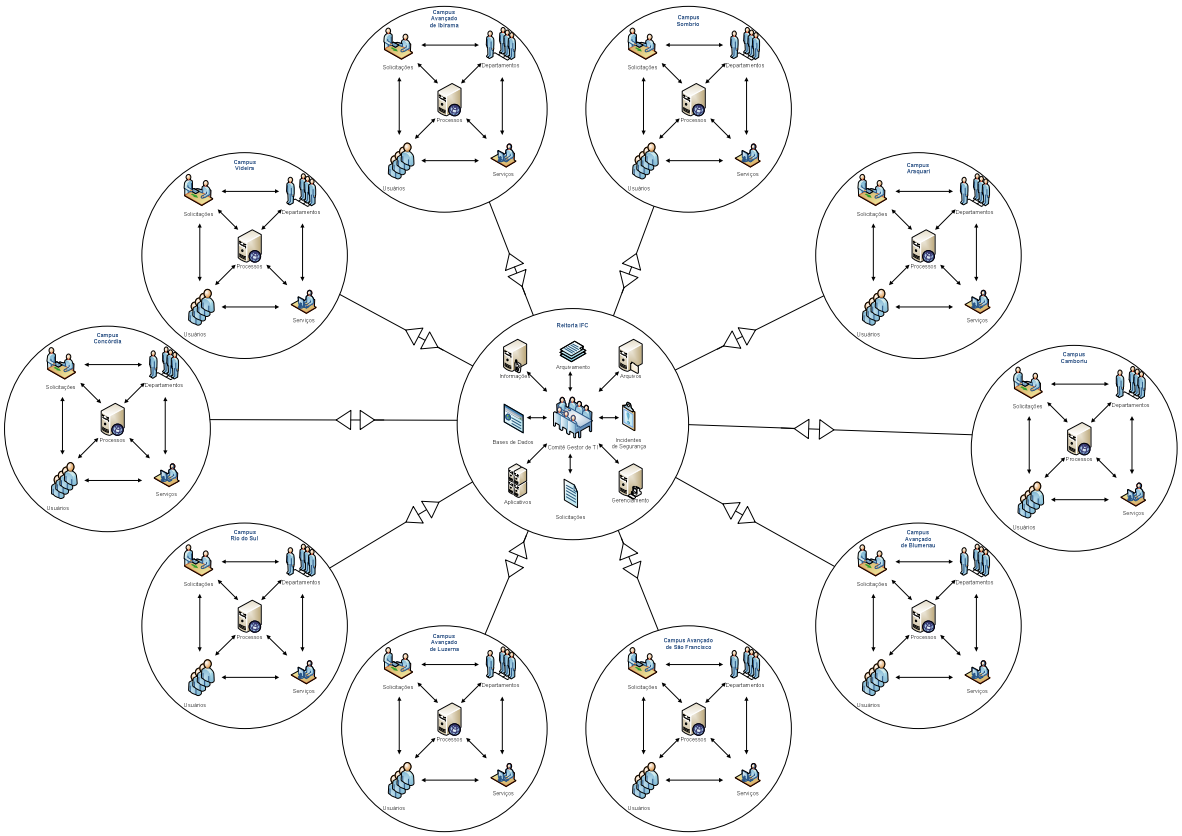

Figura 07: Sugestão de modelo de processo a ser utilizado no IFC

Fonte: Acervo do Auto

Para a implementação de sistema que realmente proporcione segurança, percebe-se que são necessárias às definições de serviços e mecanismos para tal, desta forma sugere-se a implantação de Identificações, que forneçam a capacidade de identificação de usuários, processos e recursos, o Gerenciamento de Chaves de Criptografia, que promova funções criptográficas implementadas em todos os serviços prestados, a Administração de Segurança, a ser implementada e controlada nos ambientes operacionais e nas diversas camadas de segurança, e os Sistemas de proteção, que representam a qualidade nas implementações de segurança adotadas.

Além disto, são necessárias que sejam executadas prevenções que impeçam a quebra das seguranças adotadas, como a Proteção das Comunicações, garantindo integridade, disponibilidade e confiabilidade das informações nos serviços, a Autenticação, verificando que realmente é o usuário que está utilizando o serviço, a Autorização, especificando e habilitando o que cada usuário pode ou não utilizar, o Controle de Acesso, verificando as permissões de cada usuário, o Não Repúdio, assegurando que os remetentes não possam negar a emissão da informação e os receptores não possam negar o recebimento da informação, e a Transação Privada, protegendo contra a perda da privacidade no que diz respeito às transações que estão sendo executadas pelo usuário.

Com a premissa de que nenhum conjunto de medidas de prevenção é totalmente perfeito, é necessário que as falhas de segurança sejam identificadas e tratadas de forma a reduzir ao máximo seus impactos, deste modo, são necessárias Auditorias, através das quais seja possível detectar e recuperar informações após a execução de algum ato indesejado, a Detecção de Intrusão e Confinamento, detectando em situações inseguras falhas na segurança possibilitando possíveis procedimentos de resposta, a Verificação da Integridade, identificando potenciais corrupções das informações e dos sistemas e o Retorno a um estado Seguro, caso tenha ocorrido alguma falha de segurança podendo voltar ao seu estado normal

de segurança.

Conforme os princípios de segurança, a implementação da disponibilidade e da integridade são obtidas pelo controle, identificação e capacidade de recuperação, a confidencialidade através da proteção das comunicações, o controle de acesso e o uso eficaz de mecanismos de privacidade e confidencialidade e a auditoria necessária para a manutenção de ações e o não repudio de transações efetuadas pelo sistema, obtendo assim a garantia da qualidade dos sistemas de informação, dependentes da forma e dos objetivos dos sistemas de segurança.

Amparados juridicamente, podemos contar ainda com a legislação brasileira, que prevê na lei 9.296/96, como sendo a primeira lei específica para o meio digital e trata basicamente do sigilo das transmissões de dados, sendo vedado a qualquer pessoa ou entidade o direito de interceptação de mensagens digitais ou telefônicas, bem como quaisquer comunicações entre dois computadores por meios telefônicos, telemáticos ou digitais, se aplicando ao furto de dados de bancos de dados, invasão e espionagem ou *sniffing*da rede e outros delitos que envolvam a manipulação de um terceiro à um conjunto de dados pertencente a outros computadores, e a lei 9.983/00, que prevê como crime a ação de divulgação de segredo, inclusive por meio da Internet tanto a sua transmissão quanto sua descoberta, sendo considerado como segredo, para efeitos da lei, senhas, dados de clientes ou quaisquer outras informações que não possam ser obtidas senão através da invasão do site, incluindo como crime ações que englobam mas não se limitam à inserção proposital de dados inválidos em bancos de dados e da construção e modificação de sistemas sem a autorização do proprietário. Ainda circulam pela câmara dos deputados um Projeto de lei, de número 89/04 que prevê condutas tipicamente do meio digital, como disseminação de vírus, invasão e pichação de sites, entre outros.

CONSIDERAÇÕES FINAIS

Mesmo com a consciência de que a integração de todos os campi do instituto é uma tarefa longa e demorada, tem-se a certeza de que ela irá acontecer, mesmo que não tenhamos uma data especifica.

Com a realização dos levantamentos e das pesquisas efetuadas durante o decorrer deste trabalho, percebe-se claramente a existência de uma grande heterogeneidade no uso de instrumentos de Tecnologia da Informação intra-campis e inter-campis.

Percebe-se ainda, uma grande variação de utilização em determinadas áreas dos departamentos dos *Câmpus*, alguns com uso intenso de recursos de Tecnologia da Informação, tentando aproveitar ao máximo o que existe disponível, enquanto que outras áreas departamentais, que poderiam possuir mais e melhores recursos aproveitados, não o fazem, e em muitas vezes até com prejuízo a realização de determinadas tarefas.

De uma forma geral, podem-se apontar determinados pontos clássicos na elaboração de um Plano Diretor de Tecnologia da Informação, como por exemplo, o levantamento do que existe, a determinação do que é necessário, o dimensionamento adequadode soluções tecnológicas e traçar um plano estratégico factível, para que, o que realmente é necessário,seja atendido com eficiência e eficácia.

Com a execução do Plano de Segurança como parte do Plano Diretor de Tecnologia da Informação dentro do Instituto em âmbito geral, é primordial para que novos investimentos sejam efetuados nesta área nos próximos anos, e vale ressaltar que é necessário, que periodicamente sejam feitas manutenções, revisões, atualizações, ajustes e novas demandas neste planejamento.

BIBLIOGRAFIA

BELTRÃO, Luiz e QUIRINO, Newton de Oliveira. Subsídios para uma teoria da comunicação de massa. São Paulo: Summus, 1986. P. 21 a 24.

BORDENAVE, Juan Díaz. O que é comunicação. S. Paulo: Brasiliense, 2002 (27a. ed.). P. 12 a 29 e 35 a 41.

DANTAS, Mario. Tecnologias de redes de Comunicação e computadores. Rio de janeiro: Axcel Books, 2002

GIOVANNINI, Giovani. Evolução na comunicação. Rio: Nova Fronteira, 1984. P. 23 a 83.

KUROSE, James F.; ROSS, Keith W.; Redes de computadores e a internet. 3 ed. São Paulo: Pearson Addison Weley, 2006.

LAUDON, Kenneth C. e LAUDON, Jane P. Sistemas de Informação Gerenciais. Prentice Hall; São Paulo, 2004.

LAUREANO, MARCOS A. P.; MORAES, PAULO E. S.. Segurança como estratégia de gestão da informação. Revista Economia & Tecnologia – ISSN 1415-451X, Vol. 8 – Fascículo 3 – P. 38-44. 2005

PETERSON, Larry L; DAVIE, Bruce S. Redes de Computadores. 3 ed. Rio de Janeiro: Elsevier, 2004

TANENBAUM, Andrew S. Redes de Computadores. 3 ed. Rio de Janeiro: Campus, 1997.

TURBAN, E. McLean, E.,Wetherbe, J. Tecnologia da informação para gestão. 3ª Edição, Porto Alegre, Bookman, 2004.