UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
TECNOLOGIA EM REDES DE COMPUTADORES

PLANO DE CONTINUIDADE APLICADO À UFC DE QUIXADÁ

MAICON CAMURÇA LOPES RABÊLO

QUIXADÁ - CE
Fevereiro de 2013

UNIVERSIDADE FEDERAL DO CEARÁ
CAMPUS QUIXADÁ
TECNOLOGIA EM REDES DE COMPUTADORES

PLANO DE CONTINUIDADE APLICADO À UFC DE QUIXADÁ

Autor
MAICON CAMURÇA LOPES RABÊLO

Orientador
DAVID SENA OLIVEIRA

Trabalho de Conclusão de curso submetido à Coordenação do Curso de Tecnologia em Redes de Computadores da Universidade Federal do Ceará como parte dos requisitos obtidos para obtenção do título de Tecnólogo em Redes de Computadores**.**

QUIXADÁ - CE
Fevereiro de 2013

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Campus de Quixadá

R348p Rabêlo, Maicon Camurça Lopes
Plano de continuidade aplicado à UFC / Maicon Camurça Lopes Rabêlo. – 2013.
72 f. : il. color. ; 30 cm.

Monografia (graduação) – Universidade Federal do Ceará, Campus de Quixadá, Curso de Tecnologias em Redes de Computadores, Quixadá, 2013.
Orientação: Prof. Dr. David Sena Oliveira
Área de concentração: Computação

1. Sistemas de computação. 2. Banco de dados – Medidas de segurança . 3. Computadores – Controle de acesso I. Título.

CDD 658.4038

SUMÁRIO

INDICE DE FIGURAS

ÍNDICE DE TABELAS

RESUMO

Cada vez mais instituições e empresas estão tornando-se dependentes dos recursos tecnológicos. Devido a esta dependência, torna-se necessário uma alta disponibilidade desses recursos. No intuito de prover a continuidade da execução de tarefas ou pelo menos diminuição do impacto causado, o Plano de Continuidade de Negócios (PCN) propõe medidas que sejam aplicadas em momentos em que não houver disponibilidade. A norma BS 25999-1 é quem descreve os elementos que devem existir em uma Gestão de Continuidade de Negócios (GCN) que é composto por seis etapas que serão seguidas neste trabalho para a construção do PCN. A primeira etapa define o escopo do trabalho, responsável pelo gerenciamento do plano e a forma que é gerenciado. A segunda etapa apresenta os processos críticos, relação de ameaças e riscos existentes, forma de tratamento dos riscos e o tempo para recuperação de cada falha. A terceira etapa apresenta os procedimentos adotados para cada ameaça identificada bem como a maneira de execução de tais procedimentos. Na quarta etapa é desenvolvido um plano de resposta para cada ameaça contendo as seguintes informações: objetivo, responsável, procedimentos adotados, execução dos procedimentos e atualização do plano. A quinta etapa é composta pela realização de testes contendo os seguintes tópicos: tipo de teste, níveis de complexidade, função de cada envolvido, pontos fortes, pontos fracos e obediência a padrões e legislação. A sexta etapa é composta pela implantação da gestão de continuidade na universidade.

ABSTRACT

Increasingly, institutions and businesses are becoming dependent on technological resources. Due to this dependence becomes necessary high availability of these resources. In order to provide continuity in the implementation of tasks or at least decrease the impact of, the Business Continuity Plan (BCP) proposes measures to be applied when there isn't availability. The standard BS 25999-1 describes the elements that must exist in a Business Continuity Management (BCM), which consists of six steps that will be followed in this work to build the NCP. The first step defines the scope of work, responsible for managing the plan and how it is managed. The second stage features critical processes, relationship threats and risks, as risk treatment and the recovery time of each failure. The third stage includes the procedures adopted for each identified threat as well as the manner of execution of such procedures. The fourth step is to develop a response plan for each threat with the following information: purpose, responsibility, procedures adopted, implementation of procedures and updating the plan. The fifth step is made by testing with the following topics: type of test, levels of complexity, each function involved, strengths, weaknesses and compliance with standards and legislation. The sixth stage consists of the implementation of continuity management at University.

INTRODUÇÃO

Nos dias de hoje a maior parte das empresas em todo o mundo utilizam equipamentos e meios tecnológicos aplicados em seu negócio, como forma de impor maior qualidade no atendimento do negócio e execução de serviços. As empresas utilizam Sistemas Computacionais (softwares) específicos que armazenam diversas informações, como por exemplo: cadastro de funcionários, clientes, produtos, realização de vendas, crediário, financeiro, dentre várias outras informações. Todas essas informações que a empresa opera são salvas no que chamamos de banco de dados e necessitam de segurança. Tudo o que a empresa representa são salvas nessas informações. Portanto, é de grande interesse das empresas que os dados, informações e/ou serviços, sejam sempre confidenciais, íntegros, disponíveis, possuam controle de acesso, autenticidade e não-repúdio.

Como consequência da alta utilização dos equipamentos tecnológicos no mundo dos negócios as empresas passam a se tornarem dependentes dos sistemas informatizados. O negócio fica totalmente dependente dos sistemas informatizados, o que pode gerar alguns problemas, pois se algum desses equipamentos sofrer algum dano e parar de funcionar, toda a empresa também poderá parar de funcionar, provocando sérios prejuízos para a organização, como impactos financeiros, operacionais e perda de imagem (reputação).

SILVA(2007. Pág.2) afirma: “falhas são inevitáveis, mas o impacto das falhas, ou seja, o colapso do sistema, a interrupção do fornecimento do serviço e a perda de dados, podem ser evitados pelo uso adequado de técnicas viáveis e de fácil compreensão”.

Para minimizar ou aniquilar o impacto causado pelas falhas é necessário a criação de um plano de continuidade em que sejam definidas as medidas que devem ser adotadas diante de um incidente.

O Plano de Desenvolvimento de Tecnologia da Informação da UFRS contém informações relativas ao Plano de Continuidade para os serviços de Tecnologia da Informação, porém seu estado atual é inexistente, ou seja, não existe nenhum plano de continuidade implantado ou desenvolvido na UFRS. Segundo o documento, em caso de desastre atingindo o Centro de Processamento de Dados o prazo estimado para retorno é de 6 meses. Porém o prazo aceitável seria de apenas 4 semanas. Durante esse período a universidade teria indisponível o acesso à internet e os sistemas computacionais utilizados (matrícula, vestibular, sistema acadêmico, etc.). A universidade aponta a necessidade de um Plano de Contingência para possibilitar o retorno em um prazo aceitável.

O objetivo geral do trabalho é propor através de uma análise dos ativos tecnológicos, medidas que possibilitem a continuidade do acesso aos serviços em momentos que não haja disponibilidade dos recursos de informação, identificando e tratando ameaças e riscos existentes na Universidade Federal do Ceará – Campus Quixadá.

As atividades principais realizadas foram:

- Uma coleta de informações sobre os ativos tecnológicos da UFC em Quixadá;
- Identificação dos riscos e ameaças (lógicas, físicas e humanas);
- Criação e teste de um planejamento de ações e medidas a serem tomadas quanto aos riscos.

No Capítulo 1, é motivado sobre a importância da implantação de um Plano de Continuidade de Negócio, suas principais etapas para construção e alguns conceitos importantes para a compreensão do trabalho. O Capítulo 2 apresenta o ciclo de melhoria contínua e as etapas do tratamento de risco. No Capítulo 3 é desenvolvido o Plano de Continuidade de Negócio e no Capítulo 4 são mostrados os resultados e conclusões obtidas com o trabalho.

1 CONCEITOS EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO

1.1 Motivação

A tecnologia evolui trazendo melhorias para o cotidiano das pessoas e das empresas. São melhorias que automatizam e facilitam as atividades das pessoas.

As empresas, visando melhorar a qualidade no atendimento aos seus clientes e a eficiência na realização de tarefas buscam medidas e ferramentas para automatização. É comum encontrar sistemas para realização de vendas, cadastro de funcionários, clientes, fornecedores, produtos, estoque, controle financeiro e compras.

Com a crescente informatização das empresas, uma série de processos de comunicação interna e externa passou a gerar dados relevantes que acabam por serem armazenados e hospedados em serviços como:

- **Banco de dados**: conjunto de dados integrados que tem por objetivo atender a uma comunidade de usuários (HEUSER, 1998);
- **Servidores web**: servidores que possuem um software para aceitar pedidos HTTP de clientes e servindo-os com respostas HTTP;
- **Servidores de e-mail**: servidores que realizam a gerência dos e-mails enviados e recebidos. Geralmente uma organização solicita um grupo de e-mails para utilização pelos usuários.

Todas as informações que são relevantes para uma empresa precisam ser protegidas. Essa proteção engloba processos, serviços, dados e infraestrutura. Segundo (CARUSO; STEFFEN, 2006), a Política de Segurança é um conjunto de diretrizes destinadas a regulamentar o uso seguro dos ativos de informações da organização. Ela regulamenta, essencialmente, serviços de segurança, que são garantias que se desejam obter para os recursos a serem protegidos. Na literatura, os seis principais recursos de segurança são:

- **Confidencialidade**: garantia de que o acesso à informação é restrito aos seus usuários legítimos (BEAL 2008);
- **Integridade**: garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida: em especial, prevenção contra criação, alteração ou destruição não autorizada de dados e informações (BEAL, 2008);
- **Disponibilidade**: garantia de que a informação e os ativos associados estejam disponíveis para os usuários legítimos de forma oportuna (BEAL, 2008);

- **Controle de Acesso**: consiste na medida mais importante para a proteção da informação, impedindo acessos não autorizados aos ativos de informação (BEAL, 2008);
- **Autenticação**: garantia de que quem se apresenta como remetente ou destinatário da informação é realmente quem diz ser (BEAL, 2008).
- **Não-repúdio ou irretratabilidade:** garantia de que o emissor ou receptor não tenha como alegar que uma comunicação bem-sucedida não ocorreu (BEAL, 2008).

Sendo os serviços web citados anteriormente (banco de dados, servidores web e servidores de e-mail), parte vital para o bom funcionamento de uma instituição, devem existir políticas que regulamentem seu uso e garantam sua disponibilidade. Caso não exista política definida ou sequer um plano de reação a incidentes, uma falha de um serviço ou perda de dados poderá provocar graves prejuízos financeiros. Por exemplo, o tempo em que um site de venda online fica inacessível gera uma imagem negativa junto aos consumidores, além dos prejuízos financeiros.

Seja uma instituição pública de ensino que possua um sistema acadêmico contendo notas de alunos. As únicas pessoas que devem possuir permissão de acesso para o lançamento das notas são os professores. Neste caso, existe uma preocupação em relação ao controle de acesso. Se algum usuário malicioso, seja ele externo ou interno, conseguir invadir o sistema e modificar alguma nota, e não for detectado a tempo, pode gerar problemas legais e abalar a credibilidade da instituição.

Em relação à garantia de disponibilidade, os motivos que podem causar a queda de um sistema são vários: desastres ambientais, acidentes físicos, falhas técnicas, falhas humanas, ataques ao sistema por crackers (invasores maliciosos), furtos, vírus, dentre outros. A segurança da informação utiliza-se de mecanismos para tentar evitar que usuários maliciosos possam acessar ou alterar recursos ilegalmente. Ela trata da segurança dos sistemas e está diretamente ligada à Política de Segurança. Pode-se dizer que a política de segurança é implementada através dos serviços de segurança e que os serviços de segurança são implementados através de mecanismos de segurança.

Se por um acaso, alguma informação relevante for perdida definitivamente em decorrência de falhas haverão graves consequências para a empresa ou instituição. Um simples roubo de equipamentos importantes da rede tais como servidores ou switchs, pode gerar um grande tempo de indisponibilidade mesmo que haja backups. Esse tempo será maior

ou menor se existir um plano de reação, que é denominado genericamente de plano de continuidade de negócio.

Como recomendação geral o mínimo que se deve ter é uma política de backup. O backup permite a restauração da informação a partir de locais de armazenamento seguros. A frequência de realizações de backup pode ser bastante diferenciada e está condicionada às necessidades da empresa. Esta frequência está diretamente relacionada com o grau de importância daquela informação e o tempo de duração que é levado para a realização de um backup.

Para propor medidas adequadas é necessário conhecer os ativos tecnológicos bem como os serviços oferecidos, a fim de identificar possíveis riscos e falhas.

O *Plano de Continuidade do Negócio* estuda e propõe medidas para serem executadas caso não haja disponibilidade dos recursos de informação, ou ainda, quando estiverem em estado crítico, a fim de possibilitar a continuidade do acesso aos serviços, tornando-os sempre disponíveis.

1.2 Termos Importantes

Existem alguns conceitos em segurança da informação que podem parecer sinônimos, mas entende-los é essencial para compreensão do trabalho.

Ativo: qualquer bem pertencente à organização que atribua um valor.

Problema: causa desconhecida de algum incidente ou de um conjunto de incidentes.

Evento: informação gerada ou tentativa de algo que não é comum.

Consequência: resultado de um evento.

Probabilidade: possibilidade de algo ocorrer.

Ameaça: perigo em potencial que pode causar dano ao sistema.

Risco: combinação de probabilidade de um evento e sua consequência (BEAL, 2008).

Vulnerabilidade: falha ou fraqueza que podem ser exploradas por ameaças.

Incidente: evento com consequências negativas resultante de um ataque bem-sucedido (BEAL, 2008).

1.3 Elementos em Gestão de Continuidade

Para auxiliar a construção de um plano de continuidade, permitir a evolução contínua e auditoria, existe uma série de normas que definem internacionalmente o que se deseja em continuidade de negócio.

A norma BS 25999-1 foi criada em 2007 visando fornecer as melhores práticas para a continuidade dos negócios com garantia de funcionalidade mínima. Descreve também, elementos chave que devem existir em uma Gestão de Continuidade dos Negócios. Segue alguns desses elementos:

- Produtos e processos críticos;
- Possíveis barreiras para os processos críticos;
- Como impor continuidade numa interrupção do(s) serviço(s);
- Resposta de emergência;
- Responsabilidades individuais dos colaboradores em um incidente;
- Procedimento de recuperação.

O ciclo de vida na Gestão de Continuidade dos Negócios é composto por seis etapas (Figura 1):

Figura 1: O ciclo de vida da Gestão de Continuidade de Negócios.
Fonte: http://www.brasiliano.com.br/blog/?p=2188, acessada em 03/06/2012.

- **Gestão do programa de Gestão de Continuidade dos Negócios**

Será definido qual será o escopo da gestão, ou seja, o que irá ser gerenciado, por quem será gerenciado e de que forma será gerenciado.

- **Entendendo a organização**

Deverá realizar uma verificação dos principais dispositivos que a instituição possui de acordo com a análise de impacto, sejam eles físicos ou lógicos. Em seguida, deve-se definir o tempo para recuperação da falha, as ameaças mais expressivas e como serão tratados os riscos.

- **Determinando a estratégia da continuidade de negócios**

A organização deverá definir quais medidas deverão ser adotadas e de que forma essas medidas serão aplicadas, quando houver uma falha, levando em consideração o tempo de recuperação e custo x benefício.

- **Desenvolvendo e implementando uma resposta de GCN**

A organização deve criar um plano de resposta aos incidentes. Esse plano deve estar de acordo com as expectativas e necessidades dos *stakeholders* (pessoas que possuem interesse na organização, influindo e sofrendo influência desta) e deve conter dados de como será o procedimento (objetivo, responsável, atualização do plano, dentre outros).

- **Testando, mantendo e analisando os preparativos de GCN**

A organização deverá testar o plano de resposta aos incidentes, por meio de uma implantação de um programa de testes. Para tanto, deve haver a conscientização da realização de treinamentos para todos os envolvidos no plano de negócio, a fim de garantir que quando seja necessário utilizar o plano de contingência, todos estejam preparados para realização de suas tarefas a que foram confiadas, de modo que o plano realmente cumpra o esperado.

Durante a realização desses testes é necessário que haja uma análise para verificar os pontos fortes e pontos fracos, para que posteriormente, este plano seja melhorado, garantindo seu pleno funcionamento. Os testes devem ser realizados incorporando as funções de cada membro e alterando o nível do teste e deve estar de acordo com padrões e com a legislação.

- **Incluindo a GCN na cultura da organização**

A implantação da gestão de continuidade dos negócios é algo muito significativo para uma organização. Para promover essa implantação é necessária a realização de testes, o que pode provocar certa resistência por parte dos usuários. Entretanto, quando são garantidos os processos de continuidade dos negócios, eles se tornam parte dos valores da gestão da organização.

1.4 Conclusão

Este capítulo apresentou uma motivação inicial sobre a importância da segurança da informação e da necessidade de um plano de continuidade de negócios. Os principais termos relacionados foram apresentados como também as principais fases para a construção e implantação de um plano de continuidade.

2 GESTÃO DOS RISCOS

2.1 Introdução

A Gestão dos Riscos é a parte do plano de continuidade que identifica e trata os riscos. É um conjunto de processos que permite às instituições identificar e implementar medidas de proteção. O objetivo é diminuir os riscos a que estão sujeitos os ativos da informação e equilibrá-los com os custos operacionais e financeiros envolvidos (BEAL, 2008).

Existem riscos de diversos tipos, por exemplo:

- Roubos de mídias de backup;
- Roubo de identidade, ocasionando danos à reputação;
- Quebras de propriedade;
- Vazamento de informações confidenciais.

Os riscos necessitam de medidas de proteção, a fim de oferecer segurança ao Sistema de Informação e ativos da organização, devendo sempre estar de acordo com a direção da empresa. Precisam ser definidos, medidos e analisados. Para proteger um ativo contra uma ameaça é necessário um investimento e nem sempre a relação custo x benefício é satisfatório. O ponto crucial é responder as seguintes perguntas: o que devo proteger e quanto eu devo gastar? Conhecer as ameaças, vulnerabilidades e impactos torna mais fácil a tomada de decisão sobre como e quanto gastar com a proteção dos dados e ativos.

2.2 Gestão como processo de melhoria contínua

A gestão de riscos, tal qual outros processos de gestão, aplica o modelo PDCA (Plan, Do, Check, Act – Planejar, Executar, Verificar, Agir).A Figura 2 apresenta este modelo, que é um ciclo de melhoria contínuo tornando os processos mais claros e ágeis.

Os passos do PDCA podem ser descritos como:

Plan (planejar): a organização precisa definir quais as estratégias e a forma como irá proceder para a realização das mesmas. Para definir essas estratégias é necessário seguir o mapeamento dos processos críticos de negócios:

- Elaboração de inventário dos principais ativos de informação;
- Análise a avaliação do risco associado a esses ativos;
- Mapeamento do ciclo de vida das principais informações;
- Identificação e análise das normas legais e internas;
- Elaboração da Política de Segurança.
- Definição da estrutura de gestão da segurança e das equipes que vão implementá-la.

Do (executar): todas as atividades planejadas serão executadas. Também é realizada a coleta de informações para análise posterior.

Check (checar ou verificar): os processos são avaliados e depois verificados de acordo com aquilo que foi planejado. Às vezes, a verificação pode estar diferente do planejado, gerando um desvio. Entretanto, deve ser verificado se sua execução foi capaz de atender as metas. Nesta etapa erros ou falhas podem ser detectadas.

Action (agir de forma corretiva): depois de realizada a verificação é realizada a correção dos desvios e falhas encontradas. Depois de aplicado a correção, aplica-se novamente o ciclo PDCA de modo a aperfeiçoar cada vez mais o sistema.

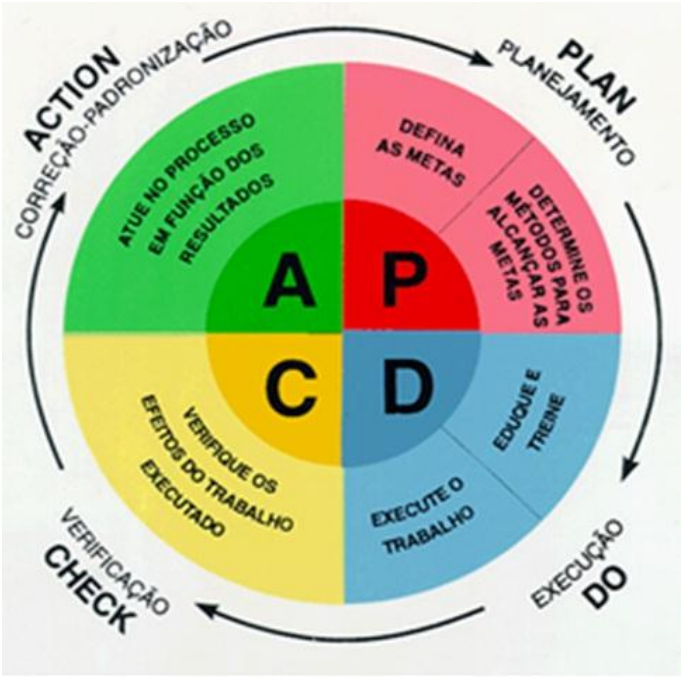


Figura 2: Ciclo PDCA.

Fonte: Adaptação de http://rehagro.com.br/plus/modulos/noticias/imprimir.php?cdnoticia=1897, acessada em 03/06/2012.

2.3 Etapas do tratamento de riscos

O documento que rege nacionalmente a gestão dos riscos é a ISO 27005. Através dele podemos obter todas as etapas do fluxograma do tratamento de risco. A Figura 3 apresenta a visão global e os processos de gestão.

Este trabalho foi desenvolvido seguindo as etapas mais importantes deste fluxograma. Em especial foram observadas as etapas de: Identificação de Riscos, Estimativa de riscos e Tratamento de Riscos.

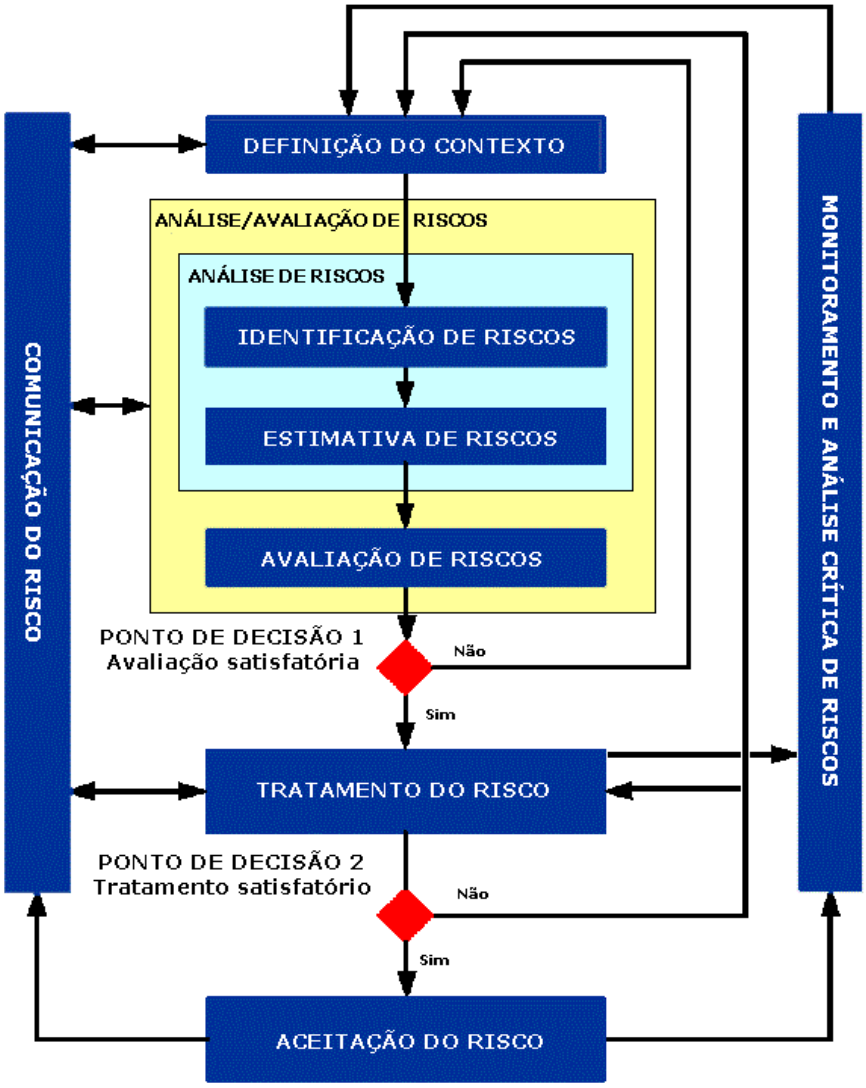


Figura 3: Processo de Gestão de Riscos de Segurança da Informação ISO 27005.
Fonte:http://www.qsp.org.br/artigo_27005.shtml, acessada em 03/06/2012.

2.3.1 Comunicação do risco

As partes interessadas (stakeholders) precisam ser informadas quanto aos aspectos dos riscos, bem como, receber e estar ciente de suas responsabilidades. É necessário também, existir uma comunicação atualizada sobre o andamento do processo da gestão de risco.

2.3.2 Definição do contexto

A definição do contexto deverá possuir um escopo da gestão de riscos (o que será implementado?). Para a criação desse escopo deverá ser realizado uma coleta de informações da organização. Essas informações devem ser principalmente sobre gestão de riscos de segurança.

O resultado da definição do contexto deverá conter as seguintes informações:

- Objetivos da Gestão de Risco;
- Ambientes contextualizados (qual ou quais ambientes?);
- Critérios na determinação dos riscos;
- Métodos para análise e avaliação dos riscos.

2.3.3 Identificação de riscos

Na identificação dos riscos deve ser descrito quais riscos serão tratados. Àqueles que não forem citados não serão analisados nem tratados. A principal função dessa etapa é determinar junto aos gestores, os eventos que podem ocasionar perdas potenciais. Para tanto, é respondido as seguintes perguntas: o que pode acontecer? Onde pode acontecer? Quando pode acontecer?

Para realização dessa etapa é necessário a identificação das ameaças, os controles existentes, vulnerabilidades e consequências.

2.3.4 Estimativa de riscos

Na estimativa de risco são gerados dados que serão utilizados para definir quais riscos serão tratados e a maneira de como será tratado, levando em consideração a melhor eficiência

de custos, bem como a probabilidade de um risco ocorrer, além do nível das consequências desse risco. Existem dois tipos de estimativas:

- Estimativa qualitativa: adota atributos qualitativos, geralmente baixos, médios e altos;
- Estimativa quantitativa: adota uma escala com valores numéricos.

2.3.5 Avaliação de riscos

Com base nos resultados da Identificação dos Riscos e na Estimativa dos Riscos, será tomada uma decisão, definindo prioridades e quais riscos possuem a real necessidade de tratamento para a importância do negócio, bem como a forma que será tratado. A avaliação do risco poderá ser usada para auxiliar a decisão de aceitar ou tratar um risco.

2.3.6 Tratamento de riscos

São medidas para modificação do risco. As medidas irão obedecer a uma ordem definida pela prioridade da probabilidade de concretização do risco. As opções de tratamento são (BEAL, 2008):

Redução do risco: ações tomadas para reduzir a probabilidade, as consequências negativas ou ambas, associadas a um risco.

Retenção do risco (aceitar): decisão de aceitar um risco.

Risco residual: risco remanescente após o tratamento do risco.

Evitação do risco: decisão de não se envolver, ou ação de fuga de uma situação de risco.

Transferência do risco: compartilhamento com um terceiro do prejuízo da perda ou benefício do ganho em relação a determinado risco (a transferência do risco pode ser feita por meio de seguros ou outros tipos de acordo).

2.3.7 Aceitação de riscos

A aceitação do risco é realizada a partir do risco residual. No momento que o responsável aceitar um risco, ele deverá assinar um registro junto com a responsabilidade pela decisão.

2.3.8 Monitoramento e análise crítica dos riscos

Os riscos são dinâmicos, podendo sofrer alterações ou acréscimo de informações. Quaisquer mudanças organizacionais ou externas podem alterar o contexto da análise. Para isso deve haver um monitoramento contínuo dos riscos e revisão de processos para identificação de oportunidade de melhoria no tratamento de riscos. Cada estágio do processo de gestão de riscos deve ser documentado.

3 APLICAÇÃO DO PCN À UFC DE QUIXADÁ

O Plano de Continuidade de Negócio (PCN) será aplicado à Universidade Federal do Ceará – Campus Quixadá. O projeto tem como objetivo principal propor medidas que possam proporcionar à rede e aos sistemas uma maior disponibilidade e segurança. O PCN baseia-se na norma **BS 25999-1** que trata da Gestão de Continuidade dos Negócios.

Todas as informações relativas ao plano de continuidade, bem como as decisões relacionadas aos riscos devem ser comunicadas à coordenação de T.I. do campus e estar de acordo com as diretrizes de segurança da universidade (em anexo).

Neste capítulo são apresentadas as etapas que foram realizadas para a construção do PCN segundo a norma citada.

Diversas métricas foram desenvolvidas para serem utilizadas como quantificadores. Elas aparecem em vários locais do PCN. Definem custo x benefício, probabilidade, consequência do risco e tempo máximo para recuperação da falha. Uma probabilidade alta da ocorrência de um evento, por exemplo, ficou definida para eventos que acontecem em média uma vez por semana. Todas as métricas desenvolvidas são parte da contribuição deste trabalho, mas foram colocadas no apêndice 5 para tornar a leitura deste capítulo mais fluída.

3.1 Etapa 01: Gestão do programa de Gestão de Continuidade dos Negócios

Esta etapa abrange os seguintes itens:

- O que será gerenciado (escopo)?
- Por quem será gerenciado?
- De que forma será gerenciado?

O que será gerenciado (escopo)?

Na universidade existem diversos recursos tecnológicos tais como: computadores, switchs, Access Point, projetores e sistemas computacionais. Os dispositivos tecnológicos da universidade que serão gerenciados serão:

- Switchs gerenciáveis de camada de rede e switchs com funcionalidades de roteamento;
- Access Point.

Por quem será gerenciado?

Como a UFC não possui política de segurança definindo como devem ser feitas as atribuições das responsabilidades, optou- se por definir como responsável o coordenador do setor de ti para o gerenciamento dos dispositivos abordados pelo PCN. Fica sob sua responsabilidade a atribuição de funções dentro do setor.

De que forma será gerenciado?

A universidade possui um software chamado Nagios que é utilizado para monitorar dispositivos e serviços. Com ele é possível saber quando os dispositivos e/ou serviços estão ativos ou não. Além disso, também é possível enviar um alerta via e-mail para o administrador da rede no instante em que houver alguma falha dos dispositivos e/ou sistemas. No entanto, considerando o escopo do trabalho ele é capaz de monitorar somente os switchs.

3.2 Etapa 02: Entendendo a organização

Esta etapa abrange os seguintes itens:

- Verificação dos dispositivos de acordo com a análise de impacto (processos críticos);
- Relação de ameaças e riscos existentes;
- Ameaças mais expressiva (ameaças e riscos que devem ser tratados);
- Como os riscos serão tratados;
- Tempo para recuperação da falha.

3.2.1 Processos críticos

Os processos críticos são todos os sistemas/serviços que são indispensáveis para o bom funcionamento da universidade.

A principal atividade que é exercida por uma universidade é a de ensino. Os professores utilizam equipamentos e serviços para realização dessa atividade. Recursos como projetor, notebook, internet e os sistemas do Campus[1]. Porém, para que o professor consiga utilizar esses recursos, faz-se necessário o uso de energia elétrica, sendo este o primeiro processo crítico para a universidade. Além dos professores, o uso da energia também é

[1] Controles de chamada, SIPPA, MOODLE, etc.

indispensável para as atividades dos servidores técnico-administrativos (tanto da secretaria como da biblioteca).

Como forma de maior controle da informação, facilidade de acesso à informação, rapidez na execução de tarefas e maior disponibilidade, a universidade utiliza os seguintes servidores:

- Servidor de Aplicação:
    - SIPPA (Sistema de Presenças e Planos de Aula);
    - SAVI (Sistema de Avaliação Institucional);
    - SISAC (Sistema de Atividades Complementares);
    - Encontros Universitários;
    - Moodle (Ambiente de Aprendizado Dinâmico);
    - Redmine (Adm. Gerenciamento de Projetos – UFC Quixadá);
    - SEven (Sistema de Eventos).
- Servidor de Arquivos;
- Servidor de Gerência de Projetos;
- Servidor HTTP, FTP, DNS, Proxy, SSH (acesso remoto);
- Servidor Nautilus (gerenciador de arquivos);
- Servidor de uso exclusivo de alguns professores que executam aplicações relacionadas a projetos de pesquisa.

Esses servidores são utilizados para a execução de várias atividades. Dentre elas:

- Realização de Frequência de alunos pelos professores;
- Upload de arquivos de aulas pelos professores;
- Postagem de notícias sobre as disciplinas pelos professores;
- Submissão de notas para alunos pelos professores;
- Lançamento de atividades complementares dos alunos por coordenadores de curso;
- Acompanhamento de aulas e frequência pelos alunos;
- Download de arquivos de aulas disponibilizadas pelos professores para os alunos;
- Solicitação de 2ª chamada de realização de provas pelos alunos;
- Envio de trabalhos pelos alunos;
- Acompanhamento de notas pelos alunos (cada aluno só é permitido visualizar sua própria nota);
- Acompanhamento de atividades complementares pelos alunos;

- Visualização da grade curricular pelos alunos;
- Avaliação institucional realizada pelos alunos;
- Fórum de discussões, a fim de solucionar dúvidas, debater sobre algum assunto referente à disciplina ou sobre a área do conhecimento do curso.

Devido ao grande uso que é feito dos sistemas e da importância que estes representam, estes também se tornam um processo crítico dentro da universidade, sendo necessário um alto índice de disponibilidade destes.

A segurança nos sistemas entraria como o terceiro processo crítico, pois constantemente os sistemas são alimentados com informações que possuem um grande valor para a universidade, como por exemplo, o lançamento de notas pelos professores. Deve-se garantir que apenas os professores tenham acesso ao lançamento e/ou alteração de notas.

Tabela 1 – Processos Críticos

Ordem	**Descrição do processo crítico**
1º processo crítico	Disponibilidade de energia elétrica para a execução de aulas pelos professores, atividades da biblioteca e secretaria da universidade.
2º processo crítico	Disponibilidade de sistemas computacionais e da rede de um modo geral.
3º processo crítico	Segurança da informação dos sistemas computacionais.

3.2.2 Relação de ameaças e riscos existentes

Nesta etapa é realizada uma lista das possíveis ameaças e riscos que podem ocorrer. Optou-se neste trabalho por seguir o *tópico 2.3.3 – Identificação de riscos*, que determina os seguintes pontos a serem observados para identificação de ameaças e riscos:

- Controles existentes;
- Vulnerabilidades;
- Consequências;
- Ameaças e riscos existentes.

3.2.2.1 Controles existentes

Controle de acesso a computadores (exceto servidores) e arquivos:

O acesso aos computadores dos laboratórios de alunos se dá por meio de usuário e senha locais. Normalmente, todos os usuários utilizam o mesmo login e senha. Qualquer tipo de documento que seja armazenado no computador fica acessível para outros usuários. Isso faz com que os usuários não utilizem os computadores da universidade para guardar arquivos pessoais, forçando-os a deixarem seus arquivos pessoais na nuvem[2].

Controle de acesso à rede e internet:

O acesso à internet se dá através de dois meios: rede cabeada e wireless. Para a rede cabeada não é necessário realizar autenticação. Basta ter acesso físico ao ponto de rede e ligar via cabo de rede o computador ao ponto de rede e este estará com acesso à rede e à internet. Para a rede wireless é utilizada apenas uma chave (senha) para ter acesso à rede e à internet.

A rede está dividida logicamente em dois grupos, bem como o acesso à internet:

- Alunos: atualmente está configurada com uma banda de 4 Mbps (upload e download);
- Administrativa: atualmente está configurada com uma banda de 2 Mbps (upload e download).

O acesso à rede dos alunos é feita através de uma senha única disponibilizada para todos os alunos. Através desta senha única o aluno pode se conectar a qualquer dos Access Point no prédio que forma a rede dos alunos. A segurança da rede é provida através do protocolo WPA2. O uso desse protocolo impede o uso de *sniffers*[3] de máquinas que estão dentro da rede, mesmo que a senha de acesso seja única.

A rede wireless administrativa também possui uma única senha de acesso que é compartilhada entre professores e servidores. A rede administrativa também é protegida pelo WPA2.

[2] Compreende-se por nuvem os serviços e aplicativos oferecidos na internet via navegador web aos usuários.
[3] O sniffer é um programa que permite que um computador receba o tráfego de outros computadores da mesma rede, mas que não estão endereçados a ele.

Controle de acesso à Sistemas e Servidores:

Todos os dados que são utilizados pela universidade são provenientes de sistemas internos e da universidade em modo geral. O acesso a esses sistemas é realizado via navegador web e se dá por meio de usuário e senha. Alunos, professores, coordenadores e servidores técnico-administrativos possuem seus diferentes níveis de acesso. No caso do servidor técnico-administrativo seu acesso varia de acordo com sua função.

Todos os sistemas internos da universidade (listados dentro do *tópico 3.2.1 – Processos críticos*) são hospedados nos servidores da universidade, sejam em Quixadá ou Fortaleza. Em Quixadá o acesso aos servidores aos quais os serviços estão hospedados é realizado através de usuário e senha local. Apenas os responsáveis pelo setor de Tecnologia da Informação possuem acesso, cada um com login e senha próprios e privilégios de super-usuário no sistema.

O controle de acesso físico à sala onde estão localizados os servidores se dá por meio de uma porta com fechadura e chave, cujas cópias são possuídas pelo responsável técnico do setor de tecnologia da informação e pela secretaria da universidade (armazenada em uma gaveta).

Para diminuir as tentativas de acesso indevido é utilizada a mudança das portas padrões de alguns serviços internos (como o SSH) num processo conhecido por *segurança por obscuridade*[4]. Um firewall limita o acesso aos serviços dependendo da rede de onde é iniciada a conexão. Além disso, são bloqueadas as portas que não são utilizadas por nenhum serviço.

Controle de acesso à dispositivos:

Todos os dispositivos estão configurados com usuário e senha, onde apenas os responsáveis pelo setor de Tecnologia da Informação do campus da universidade possuem acesso. A senha dos dispositivos é trocada, em média, apenas uma vez por ano ou quando é detectado algum acesso não autorizado ao dispositivo. Dentre os dispositivos estão:

- Switch’s;
- Access Point (senha de acesso ao dispositivo e senha de acesso à internet).

[4] Segurança por obscuridade: quando o atacante não conhece as configurações do sistema, dificultando o acesso não autorizado.

Controles contra falta de energia:

O prédio do campus universitário da UFC em Quixadá, foi construído a menos de 2 anos, possuindo, assim, instalações elétricas novas. No prédio, oscilações e quedas de energia são comuns. O campus possui 2 nobreaks que são utilizados na sala de telemática para o uso de servidores e equipamentos de rede. Os demais dispositivos não possuem nobreak, ficando indisponíveis na ausência de energia. Qualquer queda de energia acarreta queda na rede da Universidade.

Controles contra incêndio:

O prédio possui instalações elétricas, hidráulicas e cabeamento de rede novas. O clima predominante em Quixadá é próprio do sertão nordestino. Desde o início das atividades da UFC em Quixadá, não existe histórico de acidentes em relação a desabamentos, inundações ou incêndios.

Na cidade de Quixadá não existe nenhuma unidade do corpo de bombeiros. A unidade mais próxima está localizada na cidade de Quixeramobim. No interior do prédio, existem diversos extintores e mangueiras com bom estado de conservação. São realizadas sempre que necessário vistorias de modo a manter o bom funcionamento destes. Se houver a necessidade de utilizá-los, foi averiguado que existem pessoas habilitadas para o uso correto dessas ferramentas.

3.2.2.2 Vulnerabilidades

Levando em consideração os processos críticos (*Tabela 1 – Processos Críticos*), o escopo do trabalho e os controles existentes na universidade, foram identificadas as seguintes vulnerabilidades:

Tabela 2 – Vulnerabilidades

Ordem	Descrição das possíveis vulnerabilidades
Vulnerabilidade 1	Autenticação ineficiente na rede administrativa. A mesma senha utilizada por todos os servidores é raramente atualizada, em média 1 vez por ano.
Vulnerabilidade 2	Política de senhas deficiente em relação aos dispositivos da universidade. A senha utilizada nos dispositivos é trocada em média a cada 6 meses. Não existe uma política formal de troca de senhas.
Vulnerabilidade 3	Ausência de sistema alternativo de energia.
Vulnerabilidade 4	Ausência de força tarefa para combate de um possível incêndio.

3.2.2.3 Consequências

A partir das vulnerabilidades listadas na *Tabela 2 – Vulnerabilidades*, serão descritas as possíveis consequências para cada vulnerabilidade caso ela seja explorada.

Tabela 3– Consequências de vulnerabilidades

Ordem	**Consequências das Vulnerabilidades**
Vulnerabilidade 1	Se um usuário não autorizado conseguir a senha da rede administrativa, ele poderá dentre outras coisas: • Acessar a rede administrativa; • Acessar página web de configuração do Access Point (o qual é necessário possuir usuário e senha para acesso do dispositivo); • Ter acesso direto aos servidores da instituição. O acesso não autorizado a servidores causaria dentre outras coisas: o Possibilidade de remoção do próprio sistema web; o Diversas alterações de dados nos servidores; o Possibilidade de alteração de notas; o Lançamento de notícias pelo atacante utilizando uma identidade falsa; o Possibilidade de inserção de atividades complementares para alunos. • Possibilidade de acesso direto às máquinas dos servidores, secretaria e biblioteca, podendo aproveitar-se de falhas nessas máquinas.

Vulnerabilidade 2	Caso o atacante descubra a senha de acesso aos dispositivos, poderá autenticar-se em vários dispositivos da rede e alterar configurações da própria rede. Para ter acesso aos Access Points da rede administrativa, primeiramente a vulnerabilidade 1 já deve ter sido explorada e o processo de autenticação comprometido. Em compensação, eles têm acesso direto aos Access Point da rede dos alunos, podendo atacá-los (acesso às configurações) com objetivo de descobrir a senha dos equipamentos da rede administrativa. Após acessar os dispositivos da rede administrativa o atacante poderá efetuar mudanças na rede, tais quais: • Alterar senha de administrador do dispositivo; • Alterar faixas de endereçamento IP; • Alterar o endereço IP do dispositivo; • Aumentar ou diminuir a quantidade do tráfego; • Criar, excluir e/ou modificar VLAN's; • Inutilização do equipamento através de configurações propositalmente mal sucedidas.
Vulnerabilidade 3	Se o fornecimento de energia ao prédio for cortado ou interrompido, todos os Switchs e Access Points da rede (com exceção aos dispositivos instalados na sala de telemática) ficarão indisponíveis, bem como todos os dispositivos conectados a estes. A ausência de energia impossibilitará as seguintes tarefas: • Execução de aulas (quando necessário o uso dos projetores); • Indisponibilidade do uso dos computadores dos laboratórios, biblioteca e secretaria do campus; • Paralisação da maior parte das atividades técnico-administrativas; • Queda da rede wireless e rede cabeada; • Impossibilidade de uso dos sistemas computacionais do campus; • Impossibilidade de uso da central telefônica da universidade, desde que a mesma não esteja ligada ao nobreak. Entretanto, o campus conta com um aparelho telefone convencional que pode ser ligado na linha do fax em caso de queda da rede elétrica.

Vulnerabilidade 4	Um incêndio no interior do campus poderá acarretar em graves prejuízos. Podemos citar a destruição de equipamentos computacionais, danos na estrutura do prédio ou danos humanos. Devido a falta de corpo de bombeiros, deve-se criar processos internos para minorar o risco de incêndio.

3.2.2.4 Ameaças e riscos existentes

Tabela 4– Relação de Ameaças/Riscos existentes

Ordem	**Descrição da Ameaça/Risco**
Ameaça 1	Possibilidade de acesso não autorizado na rede cabeada e wireless da rede administrativa.
Ameaça 2	Possibilidade de acesso não autorizado aos Access Point e Switchs da rede administrativa.
Ameaça 3	Falha na rede elétrica.
Ameaça 4	Incêndio.

3.2.3 Ameaças mais expressiva (ameaças e riscos que devem ser tratados)

A partir da relação de todas as possíveis ameaças e riscos existentes, devem ser definidas quais ameaças/riscos mais expressiva (ameaças e riscos que devem ser tradados) que podem ocorrer na universidade. Para a realização desta etapa, serão seguidos como base os *tópicos 2.3.3 – Identificação de riscos* e 2.3.4 – *Estimativa de riscos*.

a) Com base no *tópico 2.3.3 – Identificação de riscos,* são respondidas as seguintes perguntas junto aos responsáveis pelo setor de tecnologia da informação, a fim de determinar os eventos que podem ocasionar perdas potenciais:
    - Onde pode acontecer?
    - Quando pode acontecer?

Tabela 5– Fatores para identificação de perdas potenciais

Ordem	Onde pode acontecer?	Quando pode acontecer?
Ameaça 1	• Portas com conexão RJ-45 instaladas no prédio que possuam acesso à rede administrativa; • Rede sem fio, através de acesso não autorizado à rede administrativa.	• Quando alguma sala que possua ponto de rede com acesso a rede administrativa estiver aberta e não possuir nenhum funcionário presente na sala, a fim de proibir o uso do ponto de rede; • A qualquer momento.
Ameaça 2	• Portas com conexão RJ-45 do Access Point ou Switchs com acesso a rede administrativa; • Rede sem fio, através de acesso não autorizado à rede administrativa.	• Quando alguma sala que possua Access Point ou Switch com acesso a rede administrativa estiver aberta e não possuir nenhum funcionário presente na sala, a fim de proibir o uso do Access Point; • A qualquer momento.
Ameaça 3	• Tomadas onde os dispositivos estão conectados;	• Durante falhas de fornecimento de energia elétrica pelo fornecedor; • Manutenções de energia internas (UFC) e externas (fornecedor); • Curtos circuitos; • Falhas em cabeamentos de energia; • Problemas no quadro geral de energia.
Ameaça 4	• Nos ambientes que conterem maior uso de energia e maior volume de cabos, sejam de rede ou elétrico.	• Durante o uso de energia, onde vários dispositivos e eletrodomés-ticos são conectados a rede elétrica do prédio.

b) Com base no *tópico 2.3.4 – Estimativa de riscos*, deve ser levado em consideração os pontos abaixo que irão auxiliar na definição de quais ameaças e riscos que serão tratados:

- Melhor eficiência de custos (custo x benefício);
- Probabilidade de um risco ocorrer;
- Consequências do risco.

A relação custo x benefício dar-se pelo custo obtido para solução do problema com o benefício resultante da normalização da ameaça.

Tabela 6 – Melhor Eficiência de Custos

Ordem	**Custo x benefício (péssimo, ruim, bom, ótimo, excelente)**
Ameaça 1	Excelente
Ameaça 2	Excelente
Ameaça 3	Bom
Ameaça 4	Ruim

Tabela 7 – Fatores para definição de ameaças/riscos que serão tratados

Ordem	**Probabilidade (baixa, média, alta)**	**Consequências do risco (leve, média, grave, gravíssima)**
Ameaça 1	Baixa	Média
Ameaça 2	Baixa	Grave
Ameaça 3	Alta	Leve
Ameaça 4	Baixíssima	Gravíssima

3.2.4 Como os riscos serão tratados

Tendo em mãos as principais ameaças e riscos que podem ocorrer, deve ser definido como cada risco será tratado com base no *tópico 2.3.6 –Tratamento de riscos*:

- Redução do risco;
- Retenção do risco (aceitar);

- Risco residual;
- Evitação do risco;
- Transferência do risco.

Tabela 8 – Tipo de tratamento da ameaça/risco

Ordem	Tipo de tratamento da Ameaça/Risco
Ameaça 1	Redução do risco.
Ameaça 2	Redução do risco.
Ameaça 3	Retenção do risco.
Ameaça 4	Retenção do risco.

3.2.5 Tempo máximo para recuperação de cada falha

Deve ser definido um tempo máximo para a recuperação de cada falha. A universidade deve impor um tempo limite para solução de cada problema de acordo com o grau de importância que o dispositivo, serviço ou sistema, representa para a universidade. Esse tempo é contado a partir do instante em que é identificado o problema.

Tabela 9 – Tempo máximo para recuperação da falha

Ordem	Tempo máximo para recuperação da falha (categoria 1, categoria 2, categoria 3, categoria 4, categoria 5)
Ameaça 1	Categoria 2
Ameaça 2	Categoria 2
Ameaça 3	Categoria 2
Ameaça 4	Incêndio pequeno: Categoria 1 Incêndio médio: Categoria 3 Incêndio grande: Categoria 4 ou 5

3.3 Etapa 03: Determinando a estratégia da continuidade de negócios

Esta etapa contém os seguintes itens:

- **Quais medidas serão adotadas?**
- **De que forma essas medidas serão aplicadas?**

3.3.1 Quais medidas serão adotadas?

Nesta etapa são definidos os procedimentos que são adotados dentro de um plano de contingência (geralmente um plano para cada evento).

Tabela 10 – Procedimentos adotados para cada ameaça

Ordem	Procedimentos a serem adotados
Ameaça 1	Verificação diária de comportamentos anômalos na rede administrativa.
Ameaça 2	Verificação semanal de configurações e de logs nos Access Point e Switchs que possuem acesso a rede administrativa.
Ameaça 3	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve repor o funcionamento da rede no momento em que o fornecimento de energia for reposto.
Ameaça 4	Identificar a gravidade de incêndio e tomar uma decisão de acordo com essa gravidade: • Foco de incêndio pequeno: apagar o fogo utilizando extintores adequados. Esta ação deve ser realizada apenas por funcionários, que saibam utilizar corretamente os extintores; • Foco de incêndio grande: acionar o corpo de bombeiros da unidade mais próxima (unidade do corpo de bombeiros de Quixeramobim). Esta ação pode ser realizada por qualquer funcionário. Depois do fogo apagado e o prédio liberado para o uso (no caso de incêndio grande, pode haver a necessidade de uma inspeção de segurança do prédio a fim de verificar a integridade do mesmo), o responsável pelo setor de Tecnologia da Informação do campus da universidade deve repor o funcionamento da rede.

3.3.2 De que forma essas medidas serão aplicadas?

Deve ser definida a forma que será realizada cada procedimento, ou seja, uma espécie de tutorial de como solucionar um problema, onde se tem disponível tanto os passos de como executar, bem como a forma de realizá-los.

Tabela 11 – Execução de cada procedimento

Ordem	Forma de realizar os procedimentos
Ameaça 1	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • Verificar comportamentos anômalos de acordo com padrões pré-estabelecidos (usuários e tráfego da rede); • A partir da análise realizada, identificar de qual porta (rede cabeada) ou de qual Access Point (rede wireless) o acesso foi realizado; • Procurar realizar de alguma forma o bloqueio do dispositivo que acessou irregularmente a rede administrativa; • Trocar a senha de autenticação da rede já que com a senha atual o acesso se encontra disponível para o atacante, entretanto, a troca dessa senha deve ser comunicada a todos os interessados antecipadamente; **Sugestões:** • Adoção de métodos de autenticação mais eficazes, como por exemplo, sistema de autenticação baseada em diretórios (LDAP, Active Directory, outros); • Criação de uma política de senhas que defina responsabilidades, ações e prazos para troca das senhas.
Ameaça 2	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • Identificar o dispositivo que está sendo atacado; • Remover o dispositivo atacado da rede; • Restaurar as configurações do dispositivo a partir do arquivo de configurações backup; • Alterar a senha de acesso ao dispositivo; • Salvar as configurações, inclusive uma versão para backup. **Sugestões:** • Criar senhas únicas para cada dispositivo; • Definir política de troca de senhas dos dispositivos; • Aumentar a segurança da forma que as senhas são armazenadas e compartilhadas entre os responsáveis da rede.

Ameaça 3	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • No instante em que o fornecimento de energia for reposto, verificar através do software Nagios, os serviços e switchs que voltaram a funcionar e principalmente os que não voltaram a funcionar, para correção do problema; • Verificar quais os Access Points que voltaram a funcionar e principalmente os que não voltaram a funcionar, para correção o problema; • Caso seja necessário realizar a troca de algum dispositivo será necessário realizar a importação de configurações para o dispositivo backup; • Instalar o novo dispositivo no local do outro; • Ligar o novo dispositivo na rede; • Realizar testes de conectividade para verificar a funcionalidade do equipamento. **Sugestão:** configurar uma rede mínima de contingência com pelos menos o firewall e um Access Point ligados aos nobreaks que permita a continuidade do acesso à internet em condições críticas.
Ameaça 4	• Se um funcionário identificar algum foco de incêndio pequeno, ele mesmo deve tentar apagá-lo utilizando-se do extintor ou mangueira de incêndio. Se a pessoa que identificou o foco de incêndio não possuir treinamento, esta deve comunicar o problema rapidamente para alguém que possua tal treinamento; • A partir do momento em que o foco de incêndio estiver controlado, o responsável pela rede deve repor o funcionamento da rede (caso tenha ocorrido alguma falha devido ao incidente) com os dispositivos disponíveis, utilizando-se se necessário dos dispositivos backups e realizar um levantamento das possíveis perdas do ambiente computacional; • Se o incêndio tomar grandes proporções, deve-se acionar o corpo de bombeiros da cidade mais próxima (já que a cidade onde o campus está instalado não possui corpo de bombeiros). Qualquer funcionário pode realizar esta tarefa.

3.4 Etapa 04: Desenvolvendo e implementando uma resposta de GCN

Esta etapa define um plano de resposta para cada incidente. Ela contém informações como:

- Objetivo:
- Responsável;
- Procedimentos adotados;
- Execução dos procedimentos;
- Atualização do plano.

Tabela 12 – Plano de resposta para a Ameaça 1

Ameaça 1	
Objetivo	Identificação de acessos não autorizados na rede administrativa.
Responsável pelo plano	Responsável pelo setor de tecnologia da informação do campus da universidade.
Procedimentos adotados	*Tabela 10*, linha "Ameaça 1"
Execução dos procedimentos	*Tabela 11*, linha "Ameaça 1".
Atualização do plano	O plano deve ser revisto a cada 3 meses, a fim de garantir a qualidade dos passos a serem seguidos, de modo a atingir o objetivo do plano.

Tabela 13 – Plano de resposta para a Ameaça 2

Ameaça 2	
Objetivo	Identificação de acessos não autorizados aos Access Point e Switchs da rede administrativa, bem como alterações de configurações.
Responsável pelo plano	Responsável pelo setor de tecnologia da informação do campus da universidade.
Procedimentos adotados	*Tabela 10*, linha "Ameaça 2"
Execução dos procedimentos	*Tabela 11*, linha "Ameaça 2".
Atualização do plano	O plano deve ser revisto a cada 3 meses, a fim de garantir a qualidade dos passos a serem seguidos, de modo a atingir o objetivo do plano.

Tabela 14 – Plano de resposta para a Ameaça 3

Ameaça 3	
Objetivo	Repor o funcionamento da rede após uma falha elétrica.
Responsável pelo plano	Responsável pelo setor de tecnologia da informação do campus da universidade.
Procedimentos adotados	*Tabela 10*, linha "Ameaça 3"
Execução dos procedimentos	*Tabela 11*, linha "Ameaça 3".
Atualização do plano	O plano deve ser revisto a cada 3 meses, a fim de garantir a qualidade dos passos a serem seguidos, de modo a atingir o objetivo do plano.

Tabela 15 – Plano de resposta para a Ameaça 4

Ameaça 4	
Objetivo	O que fazer diante de um incêndio.
Responsável pelo plano	1ª parte: qualquer funcionário que possua treinamento para a correta utilização de extintores de incêndio; 2ª parte: responsável pelo setor de tecnologia da informação do campus da universidade.
Procedimentos adotados	*Tabela 10*, linha "Ameaça 4"
Execução dos procedimentos	*Tabela 11*, linha "Ameaça 4".
Atualização do plano	O plano deve ser revisto a cada 6 meses, a fim de garantir a qualidade dos passos a serem seguidos, de modo a atingir o objetivo do plano.

3.5 Etapa 05: Testando, mantendo e analisando os preparativos de GCN

- **Teste via programa de testes;**
- **Definição de pontos fortes;**
- **Definição de pontos fracos;**
- **Função de cada envolvido;**
- **Nível de complexidade;**
- **Respeitar padrões e legislação.**

Nesta etapa do projeto, o plano é testado de modo a verificar se ele realmente pode ser colocado em prática de forma que atenda ao esperado. Um dos objetivos na realização dos testes é o ajuste dos procedimentos através da observação dos pontos fracos. A cada ciclo é aperfeiçoado o plano de continuidade e novos testes validam novos procedimentos.

Tabela 16– Testes Ameaça 1

Tipo de teste	Testes de mesa, através da verbalização dos procedimentos de recuperação para diferentes formas de interrupção para cada plano.
Níveis de complexidade	**Nível 1:** detectado acesso não autorizado à rede administrativa via wireless através do monitoramento da rede.
Função de cada envolvido	Responsável pelo setor de tecnologia da informação do campus da universidade. **Nível 1:** • Verificação de comportamentos anômalos na rede administrativa; • Bloquear o dispositivo que realizou o acesso; • Trocar a senha de autenticação da rede administrativa.
Pontos fortes	**Nível 1**: não é frequente a necessidade de verificação de logs.
Pontos fracos	**Nível 1**: um dos objetivos do atacante talvez seja tentar conseguir acesso aos servidores. Como a identificação de usuários não autorizados na rede administrativa se dá basicamente por comportamentos anômalos, o atacante poderia fazer uso da rede de acordo com a média utilizada, ou seja, não provocar esses comportamentos. Com isso se torna necessário um processo de autenticação mais eficaz, a fim de evitar acessos não autorizados.
Respeitar padrões e legislação	Os procedimentos adotados não contrapõem a legislação.

Tabela 17– Testes Ameaça 2

Tipo de teste	Testes de mesa, através da verbalização dos procedimentos de recuperação para diferentes formas de interrupção para cada plano.
Níveis de complexidade	**Nível 1:** identificado acesso não autorizado ao Access Point ou Switch da rede administrativa com realização de alterações nas configurações.
Função de cada envolvido	Responsável pelo setor de tecnologia da informação do campus da universidade. **Nível 1:** Restaurar as configurações do dispositivo a partir de um arquivo de configurações backup e alterar a senha de acesso.
Pontos fortes	**Nível 1:** o processo de recuperação das configurações originais dos dispositivos é rápido.
Pontos fracos	**Nível 1:** o acesso aos dispositivos se restringe a usuário e senha, permitindo novas possibilidades de ataques.
Respeitar padrões e legislação	Os procedimentos adotados não contrapõem a legislação.

Tabela 18– Testes Ameaça 3

Tipo de teste	Testes de mesa, através da verbalização dos procedimentos de recuperação para diferentes formas de interrupção para cada plano.
Níveis de complexidade	**Nível 1:** queda de energia de até 2 horas; **Nível 2:** queda de energia acima de 2 horas (capacidade do nobreak não suportada).
Função de cada envolvido	**Nível 1 e Nível 2:** • **Qualquer funcionário**: acionar a empresa fornecedora de energia através de telefone; • **Responsável pelo setor de tecnologia da informação do campus da universidade:** verificar os dispositivos que não voltaram a funcionar após a correção da falha de energia elétrica.
Pontos fortes	**Nível 1 e Nível 2:** no momento em que a energia for resposta, a verificação dos switchs que voltaram e não voltaram a funcionar é bastante rápida devido a utilização de software específico de gerenciamento e monitoramento.
Pontos fracos	**Nível 1 e Nível 2:** • Praticamente todos os recursos tecnológicos ficariam indisponíveis durante a falta de energia, impossibilitando, muitas vezes, a realização de aulas; • Verificação manual dos Access Point que voltaram e não voltaram a funcionar.
Respeitar padrões e legislação	Os procedimentos adotados não contrapõem a legislação.

Tabela 19– Testes Ameaça 4

Tipo de teste	Testes de mesa, através da verbalização dos procedimentos de recuperação para diferentes formas de interrupção para cada plano.
Níveis de complexidade	**Nível 1:** foco de incêndio pequeno. **Nível 2:** incêndio grande.
Função de cada envolvido	**Nível 1:** • **Funcionário que possua conhecimento sobre o correto uso de extintores e mangueiras de incêndio**: utilizar extintores e/ou mangueiras de incêndio (dependendo da situação) para inibir o fogo; • **Responsável pelo setor de tecnologia da informação do campus da universidade:** repor o funcionamento da rede após o incidente. **Nível 2:** • **Qualquer funcionário**: acionar o corpo de bombeiros da cidade mais próxima; • **Responsável pelo setor de tecnologia da informação do campus da universidade:** repor o funcionamento da rede após o incidente e prédio liberado para uso.
Pontos fortes	**Nível 1:** existem funcionários qualificados para o correto uso dos equipamentos contra incêndio e os equipamentos estão sempre em boas condições de uso; **Nível 2:** facilidade em acionar a unidade do corpo de bombeiros (via telefone ou celular pelo número 193).
Pontos fracos	**Nível 1:** nem todos os funcionários possuem treinamento contra incêndio; **Nível 2:** • Não existe unidade do corpo de bombeiros na cidade onde o campus Quixadá está instalado, provocando grandes prejuízos para a universidade; • Dificuldade para repor o funcionamento da rede devido a possíveis perdas de equipamentos (inclusive os equipamentos backup), além de possíveis falhas nos cabeamentos elétricos e de rede.
Respeitar padrões e legislação	Os procedimentos adotados não contrapõem a legislação.

3.6 Etapa 06: Incluindo a GCN na cultura da organização

- Implantação da gestão de continuidade dos negócios na universidade inclui:
    - Comprometimento das pessoas envolvidas;
    - Reconhecimento da importância da GCN.

Para promover a conscientização da importância do plano de continuidade de negócio serão realizadas palestras sobre como essas medidas são importantes para a universidade, de forma a criar um espírito de comprometimento e responsabilidade nas pessoas.

4 CONCLUSÃO

Diante do cenário que se encontra as universidades, instituições e organizações perante a dependência do uso da tecnologia, se torna imprescindível o desenvolvimento de um plano de continuidade onde são descritas quais os principais riscos e ameaças que podem ocorrer e como evitar ou solucionar tais problemas. Com isso, a recuperação se torna bem mais rápida, fator determinante em um negócio. A partir de um plano de continuidade já montado, a recuperação de um incidente se torna muito mais rápido e controlado, pois as pessoas envolvidas para a solução do problema já sabem exatamente o que devem fazer e como fazer. Quanto mais abrangente for o plano de continuidade, ou seja, quanto maior a quantidade de problemas mapeados, maior será sua eficiência.

Riscos existem vários e custa dinheiro para serem tratados, por isso se torna importante realizar uma boa avaliação dos principais riscos (por exemplo, aqueles que ocorrem com maior frequência e que possuem consequências graves) para decidir quais devem ser tratados. Às vezes, pode valer apena tratar um risco que dificilmente irá acontecer, mas que sofrerá grandes consequências negativas se ocorrer.

Um problema identificado na execução dos procedimentos foi a permanência da possibilidade de acesso não autorizado na rede administrativa wireless, a qual o único processo de autenticação é a senha da rede. Com o acesso indevido a rede administrativa é criada possibilidades de acesso aos servidores o que causaria sérios problemas para a universidade. É importante notar que é através de uma falha no início do processo de autenticação da rede administrativa que vai sendo gerada uma “bola de neve” com possibilidades de o atacante acessar e modificar todos os sistemas hospedados no campus Quixadá. Perante essas consequências no processo de autenticação existente, se tornaria necessário uma adoção de novas formas de autenticação, como por exemplo, sistema de autenticação baseada em diretório (LDAP, Active Directory, dentre outros).

Um segundo problema identificado na execução dos procedimentos é a ausência de fontes alternativas de energia. Diante de problemas como falta de energia a universidade fica quase que totalmente sem condições de uso da rede e até mesmo das atividades exercidas pela secretaria da universidade e realização de aulas. Perante essas consequências da falta de energia, se tornaria necessário uma adoção de medida onde existisse uma fonte de energia alternativa para os momentos em que houvesse essas falhas.

Um terceiro problema identificado na execução dos procedimentos é a ausência de uma unidade do corpo de bombeiros na cidade de Quixadá. Se um incêndio tomar grandes

proporções no campus universitário a destruição de equipamentos e de instalações elétrica e de rede serão desastrosas, pois o tempo para a chegada do corpo de bombeiros ao local do incêndio será muito grande em relação a velocidade de propagação de incêndio.

Embora, muitas vezes os procedimentos executados não propiciam a continuidade do negócio, ao menos eles conseguem minimizar o impacto causado e dão maior velocidade no processo de recuperação. Enfim, quando se tem os problemas mapeados com suas respectivas soluções e com pessoas preparadas para agir diante de um incidente, o impacto causado se torna bem menor.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2007:** Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2007.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27005:2008:** Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação. Rio de Janeiro, 2008.

BEAL, Adriana. **Segurança da informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. 1ª Edição São Paulo: Atlas, 2008.

BRITISH STANDARDS INSTITUTE. **BS 25999-1**: Code of Practice for Business Continuity Management. London, 2006.

CARUSO, Carlos; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. 3.ed. São Paulo: Senac, 2006.

COBIT – Modelo de Maturidade. São Paulo, 2000. Disponível em: <www.madah.com.br/Cobit_Modelo_Maturidade.doc>. Acesso em: maio/2012.

FAGUNDES, E. M. **COBIT: um kit de ferramentas para a excelência de TI.** São Paulo, 2004. Disponível em: <http://www.efagundes.com/artigos/COBIT.htm>. Acesso em: maio/2012.

HEUSER, Carlos Alberto. **Projeto de Banco de Dados**. 4. ed. Porto Alegre: Sagra Luzzatto, 2001. (Livros Didáticos).

MAGALHÃES, I. L.; PINHEIRO W. B. **Gerenciamento de Serviços de TI na prática: Uma abordagem com base no ITIL**. Porto Alegre: Novatec, 2007.

RIGON, Evandro Alencar; WESTPHALL, Carla Merkle. **Modelo de Avaliação da Maturidade da Segurança da Informação**. VII Simpósio Brasileiro de Sistemas de Informação. Salvador, Bahia, 2011. Departamento de Informática e Estatística (INE). Universidade Federal de Santa Catarina (UFSC).

SILVA, Ronaldo; MOURA, Viviane da Cunha; DEPONTI, Euclides; ROSA, Vinícius. **Plano de Continuidade de Negócios Planejamento**. Artigo publico em lyfreitas.com.br. Universidade Católica de Brasília (UCB), 2007. Brasília DF. Coordenação de Pós Graduação.

Universidade Federal do Rio Grande do Sul. **Plano de Desenvolvimento de tecnologia de Informação (PDTI)**. Disponível em: <http://www.ufrgs.br/ufrgs/a-ufrgs/pdti-plano-diretor-de-tecnologia-da-informacao>. Acesso em: fevereiro/2013.

APÊNDICE 01 – Questionário sobre a Estrutura de TI da UFC-Quixadá

Questionário a ser aplicado aos responsáveis pelo setor de TI, Zarathon Maia e Jeandro Mesquita com o objetivo de conhecer os recursos, processos e necessidades do setor de TI.

As informações requisitadas serão utilizadas para fins acadêmicos para elaboração dos procedimentos de um trabalho de conclusão de curso do aluno Maicon Camurça Lopes Rabêlo, matrícula 0317584, que possui como tema "Plano de Continuidade de Negócio aplicado à UFC de Quixadá". Tem como Orientador o professor doutor David Sena Oliveira. A monografia gerada utilizando-se dessas informações será publicada somente se obtiver aprovação do Coordenador de TI do Campus UFC – Quixadá, sendo obrigado o aluno a excluir da monografia as informações então vetadas.

SERVIDOR

- **Quantos servidores existem?**

  R.: 6 servidores.

- **Quais serviços cada servidor hospeda~~m~~?**

  R.: Nautilus (gerenciador de arquivos)

  HTTP, FTP, DNS, Proxy, SSH (acesso remoto)

  Servidor de aplicação TomCat (servidor de aplicação Java), apache com php

  Servidor de arquivos

  Gerência de projetos

  Servidor Chríston (roda suas aplicações)

- **Quem possui acesso aos servidores e suas configurações?**

  R.: Zarathon, Jeandro, Marcos Dantas e João Marcelo.

- **Como se dá o controle de acesso a servidores? Apenas usuário e senha?**

  R.: Usuário e senha. Cada administrador possui seu usuário e senha com privilégios de ROOT em cada servidor.

- **Em relação à segurança, é utilizado bloqueio de portas, por exemplo?**

  R.: Como regra**, são bloqueadas** todas as portas e liberadas somente as portas necessárias para o uso. Também são utilizadas portas não padrão.

- **Que outras medidas são adotadas para a segurança?**

  R.: É utilizado um proxy com firewall onde todas as portas são bloqueadas com exceção àquelas que são utilizadas pelos servidores.

ACESSO À REDE E INTERNET

- **Qual o link disponível (velocidade)? Link dedicado?**

  R.: Link dedicado de 6 Mbps fornecido pela Bayde Net, sendo 6Mpbs de Upload e 6 Mbps de Download.

- **Como é dividida a rede da internet (divisão de link em grupos de usuários)?**

  R.: O uso da internet é dividida em 2 grupos: aluno (4 Mbps) e servidores (2 Mbps).

- **Como se dá a autenticação na rede?**

  R.: Rede cabeada não possui autenticação. Rede Wireless possui autenticação através de senha.

- **A cobertura de sinal é capaz de cobrir todo o prédio para todos os grupos de usuários?**

  R.: Sim. A rede sem fio é capaz de cobrir todos os pontos do prédio para ambos os grupos de usuário (aluno e servidor).

- **Existe interferência na rede sem fio? Qual o motivo dessa interferência?**

  R.: Sim. Existe interferência na rede sem fio. Isso se dá devido a pouca quantidade de canais disponíveis. Como os canais ficam uns próximos dos outros, isso acaba gerando interferência nos roteadores.

- **Quem tem acesso às configurações dos pontos de acesso?**

  R.: Zarathon, Jeandro, João Marcelo e Marcos Dantas.

- **Existem pontos de acesso backup na universidade? Quantos?**

  R.: Sim. Existem 8 roteadores backup. Para cada dispositivo existe um arquivo backup com todas as configurações salvas, de modo que se algum dispositivo falhar é realizado a restauração do arquivo backup para o roteador backup.

ACESSO AOS COMPUTADORES

- **Como se dá o acesso aos computadores?**

  R.: Apenas usuário e senha local. *(Única e senha para todos os usuários)*

- **Quantos tipos de usuários para acesso aos computadores existem? Quais são?**

  R.: Os usuários são configurados em cada máquina, ou seja, não existe um usuário e senha padrão capaz de utilizar todas as máquinas da universidade. Entretanto, de uma forma geral (usuário e senha local) são utilizados os seguintes tipos de usuários: administrador, aluno e servidor (onde cada um vai ter um usuário e senha que desejar no computador que utiliza).

- **Como são atribuídos os direitos de acesso (quem tem acesso ao quê)?**

  R.: Os direitos de acesso são atribuídos através de sub-redes. São utilizados dois tipos de sub-redes: aluno e servidor. **Rede dos alunos:** não conseguem conectar uma maquina a outra, podem realizar um ping somente com outra maquina da mesma rede e não possuem acesso às configurações. **Rede dos Servidores:** possuem acesso a arquivos compartilhados, serviços próprios da administração.

DISPOSITIVOS

- **SWITCH**
  - **Quais os tipos de switch's utilizados na rede (layer 2, layer 3, outros)?**

    R.: Layer 2 e Layer 3.

  - **Qual a quantidade que está sendo utilizada?**

    R.: Cada laboratório (4 laboratórios no total) possui 3 switch's layer 2 e na sala de telemática possui 5 switch's layer 2 e 1 switch layer 3.
    Layer 2 → (4x3) + 5 = 12+5 = 17.
    Layer 3 → 1.

  - **Quantos switch's backup existem (especificando o tipo de switch)?**

    R.: 3 switch's layer 3 e 3 switch's layer 2.
    Para cada dispositivo existe um arquivo backup com todas as configurações salvas, de modo que se algum dispositivo falhar é realizado a restauração do arquivo backup para o roteador backup.

- **ROTEADOR**
  - **Quais os tipos de roteador são utilizados na rede (incluindo velocidade, capacidade de usuários, distância de transmissão)?**

    R.: Roteadores da Apple (AirPortExtreme). Esses roteadores permitem plugar impressora, HD (disponibilizando arquivos numa rede). Trabalham nas bandas "a", "b", "g", "n" e nas frequências 5 MHz e 2.4 MHz.

  - **Qual a quantidade de roteadores está sendo utilizada?**

    R.: 6 roteadores, sendo: 3 para alunos e 3 para servidores.

  - **Quantos roteadores backup existem (especificando as características já citadas)?**

    R.: 2 roteadores backup também da Apple com as mesmas especificações.

- **É utilizada alguma forma de gerenciamento dos dispositivos?**

  R.: Sim. É utilizado o Nagios que é um software de monitoramento tanto para dispositivos como serviços. Com ele é possível saber quando os dispositivos (switchs) estão ativos ou não. Além disso, através dele é possível enviar um alerta caso algum dispositivo ou serviço fique inativo. No nosso caso é enviado um e-mail para o responsável da rede.

- **Existe alguma proteção de acesso à dispositivos? Como se dá essa proteção?**

  R.: Apenas usuário e senha dos dispositivos, além do acesso à rede do grupo de usuário dos servidores, pois para ter acesso à tela de login dos dispositivos é necessário estar na mesma rede do grupo dos servidores.

- **Quem pode visualizar e/ou alterar tais configurações?**

  R.: Os administradores da rede: Zarathon, Jeandro, João Marcelo e Marcos Dantas.

- **NOBREAK**
  - **Quantos nobreaks estão em uso na universidade?**

    R.: 2 nobreaks com potencias diferentes.

  - **Para qual fim são utilizados?**

    R.: O nobreak com potência maior atende ao consumo de todos os servidores. O nobreak com potência menor atende ao consumo de todos os switch's concentrados na sala de telemática.

  - **Qual a autonomia de cada um?**

    R.: Nobreak de potência maior: 4 horas;

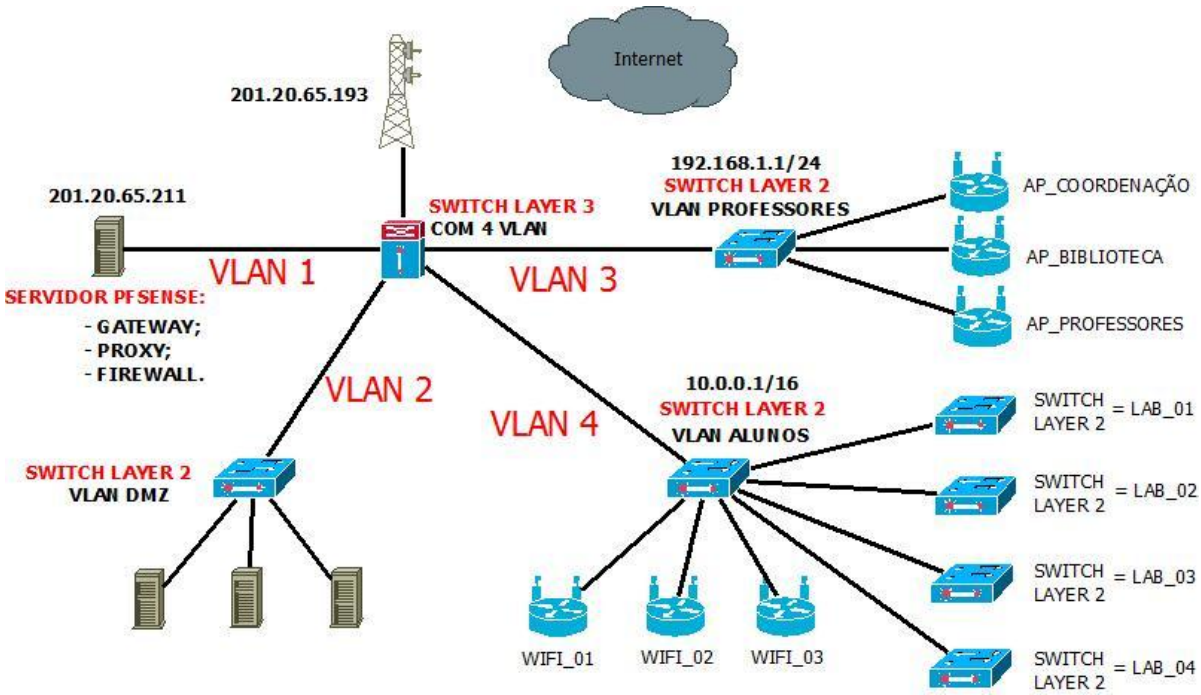
    Nobreak de potência menor: uma hora e meia a duas horas**.**

- **Existem nobreaks backup? Qual a autonomia de cada um?**

  R.: não existe nobreak backup.

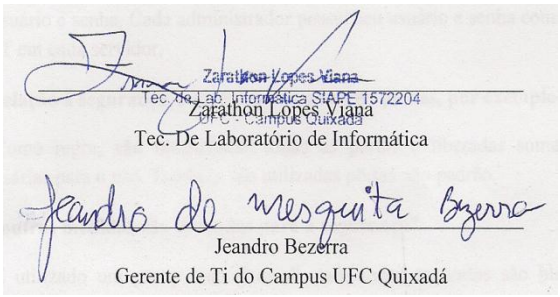
TOPOLOGIA DA REDE

- **Qual a topologia da rede?**



- **Se algum dispositivo falhar, o serviço será interrompido? Ou existe alguma alternativa?**

  R.: Depende. Se um switch falhar, toda a rede a qual ele estiver conectando também irá cair. Não existe uma rota redundante. Ponto crítico da rede: switch master que é responsável pela gerência de todos os servidores e da rede interna. Se o switch master cair, toda a rede, inclusive os servidores, ficaria sem funcionar.



APÊNDICE 02 – Questionário sobre os incidentes de queda na rede elétrica

As informações requisitadas serão utilizadas para fins acadêmicos para elaboração dos procedimentos de um trabalho de conclusão de curso do aluno Maicon Camurça Lopes Rabêlo, matrícula 0317584, que possui como tema "Plano de Continuidade de Negócio aplicado à UFC de Quixadá", que tem como Orientador o professor doutor David Sena Oliveira.

A monografia gerada utilizando-se dessas informações será publicada somente se obtiver aprovação do Coordenador de TI do Campus UFC – Quixadá, sendo obrigado o aluno a excluir da monografia as informações então vetadas.

Questionário aplicado ao Servidor Técnico Administrativo Jones Almeida.

Data de realização da entrevista: 01/02/2013.

- **Qual a data de inauguração do prédio?**

  R: 26 de março de 2012.

- **Qual a empresa fornecedora de energia elétrica?**

  R: Coelce.

- **Com que frequência (mensal) ocorre falhas ou quedas de energia no prédio (seja interno ou externo)?**

  R: Frequentemente têm ocorrido quedas de energia. Praticamente quase todos os dias da segunda quinzena do mês de janeiro/2013, mas em fevereiro ainda não têm ocorrido quedas de energia.

- **Qual o principal motivo de quedas de energia no prédio?**

  R: Um equipamento obsoleto da empresa fornecedora de energia elétrica localizada em um ponto próximo ao campus, sendo, assim, um problema externo. Tal equipamento tem se tornado obsoleto de acordo com o aumento do uso de energia pelos clientes da empresa fornecedora de energia elétrica, dentre eles IFCE e UFC.

- **Quando o fornecedor de energia elétrica realiza alguma manutenção de energia de modo que o fornecimento desta seja interrompido, a universidade (campus Quixadá) é informada antecipadamente de que o processo será realizado?**

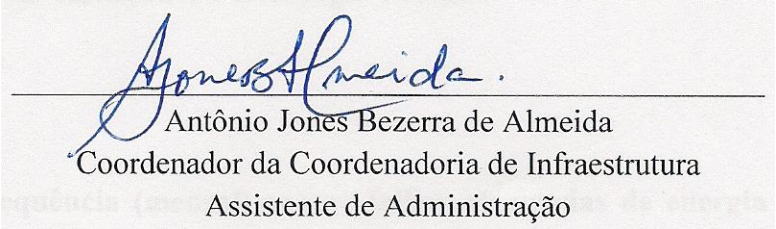
  R: Até o presente momento nunca recebemos nenhum comunicado por parte da empresa fornecedora de energia elétrica.

- **Quando ocorre alguma manutenção de energia (interna) no prédio a secretaria do campus ou algum outro funcionário é informado com antecedência?**

R: Sim, sempre que for ocorrer alguma atividade de manutenção a COP – Coordenadora de Obras e Projetos, localizada no campus de Fortaleza, avisa antecipadamente.

- **Com que frequência é realizada a manutenção de energia (interna)? Como se dá esse processo?**

R: Sempre que ocorrer alguma necessidade o setor responsável (que fica localizado em Fortaleza) é comunicado através do campus Quixadá. Além disso, são realizadas vistorias em média 1 vez por ano.


Antônio Jones Bezerra de Almeida
Coordenador da Coordenadoria de Infraestrutura
Assistente de Administração

APÊNDICE 03 – Questionário sobre segurança no trabalho

As informações requisitadas serão utilizadas para fins acadêmicos para elaboração dos procedimentos de um trabalho de conclusão de curso do aluno Maicon Camurça Lopes Rabêlo, matrícula 0317584, que possui como tema "Plano de Continuidade de Negócio aplicado à UFC de Quixadá", que tem como Orientador o professor doutor David Sena Oliveira.

A monografia gerada utilizando-se dessas informações será publicada somente se obtiver aprovação do Coordenador de TI do Campus UFC – Quixadá, sendo obrigado o aluno a excluir da monografia as informações então vetadas.

- **Existe alguém responsável pela manutenção dos extintores? Qual a função/cargo atribuída a ela atualmente?**

R: Existe um departamento no campus de Fortaleza chamado Departamento de Atividades Auxiliares – DAA. Quando ocorre alguma necessidade a coordenadoria de Infraestrutura do Campus Quixadá envia um ofício com a solicitação para o DAA. Geralmente quando se trata de troca ou recarga, os funcionários do DAA trazem equipamentos preparados e levam os equipamentos que estão inaptos para o uso. A função atribuída por este funcionário em Fortaleza é Diretor da Divisão de Vigilância e Segurança.

- **No prédio existem extintores e mangueiras de incêndio. Ambos os equipamentos funcionam?**

R: Sim, ambos estão aptos para o uso. Testes já foram realizados.

- **Os funcionários possuem algum treinamento de como reagir diante de um incêndio seja este pequeno ou grande?**

R: Sim, foi realizado um treinamento há aproximadamente 4 meses. O treinamento foi promovido por funcionários do DAA tendo como alunos os vigilantes, funcionários da manutenção e de serviços gerais do campus Quixadá. Lembrando que sempre deve ser protegida a integridade física do funcionário, não podendo então, fazer uso dos extintores em ocasiões arriscadas o que colocaria a integridade física em risco.

- **Existem basicamente três tipos de extintores: CO2, Água e Pó Químico. Quando usado um tipo de extintor errado às vezes pode aumentar mais ainda o fogo. Diante de um incêndio pequeno qual a medida a ser adotada pelos funcionários?**

R: Inicialmente deve tentar apagar o fogo (de forma segura) e posteriormente acionar o corpo de bombeiros.

- **Com que frequência é realizada a troca ou reabastecimento dos extintores presentes no prédio?**

R: Anual ou dependendo da validade do extintor.

Antônio Jones Bezerra de Almeida
Coordenador da Coordenadoria de Infraestrutura
Assistente de Administração

APÊNDICE 04 – Questionário sobre a política de senhas

As informações requisitadas serão utilizadas para fins acadêmicos para elaboração dos procedimentos de um trabalho de conclusão de curso do aluno Maicon Camurça Lopes Rabêlo, matrícula 0317584, que possui como tema "Plano de Continuidade de Negócio aplicado à UFC de Quixadá", que tem como Orientador o professor doutor David Sena Oliveira.

A monografia gerada utilizando-se dessas informações será publicada somente se obtiver aprovação do Coordenador de TI do Campus UFC – Quixadá, sendo obrigado o aluno a excluir da monografia as informações então vetadas.

O objetivo deste questionário é obter junto ao responsável pelo Setor de TI a atual Política de senhas e desenvolver procedimentos de execução de solução de problemas que sejam adequados às necessidades da Universidade.

TROCA DE SENHA:

- **Existe alguma política de troca de senha?**

R: Não. As senhas são trocadas, porém não obedecem a nenhum tipo de controle ou padrão.

- **Com que período é realizado a troca de senha de acesso dos dispositivos?**

R: Geralmente são trocadas a cada 6 meses, porém não existe nenhum controle sobre essa troca. Eventualmente quando alguém descobre a senha ou o setor de TI acha que está no momento de trocar a senha, então esta senha é trocada, entretanto, não existe nenhum controle sobre essas trocas, não existe nada definido e nenhum planejamento.

- **Com que período é realizado a troca de senha de acesso aos servidores?**

R: Como cada administrador possui um login e senha para acesso ao servidor cada um fica responsável por sua senha, não tendo nenhuma definição ou obrigação sobre a periodicidade de troca dessa senha. Existe um usuário que é utilizado em todos os servidores onde sua senha é trocada em média 1 vez ao ano (não possuindo nada organizado ou planejado).

- **Com que período é realizado a troca de senha de acesso à rede administrativa wireless?**

R: Em média é realizada uma troca a cada 6 meses ou 8 meses. Também não possui nenhum controle sobre essa troca de senha.

- **Levando em consideração a *Tabela 4– Relação de Ameaças/Riscos existentes*, preencher as tabelas:**

    - **Tabela 10 – Procedimentos adotados para cada ameaça;**
    - **Tabela 11 – Execução de cada procedimento.**

Tabela 4– Relação de Ameaças/Riscos existentes

Ordem	Descrição da Ameaça/Risco
Ameaça 1	Possibilidade de acesso não autorizado na rede cabeada e wireless da rede administrativa.
Ameaça 2	Possibilidade de acesso não autorizado aos Access Point e Switchs da rede administrativa.
Ameaça 3	Falha na rede elétrica.
Ameaça 4	Incêndio.

Tabela 10 – Procedimentos adotados para cada ameaça

Ordem	Procedimentos a serem adotados
Ameaça 1	Verificação diária de comportamentos anômalos na rede administrativa.
Ameaça 2	Verificação semanal de configurações e de logs nos Access Point e Switchs que possuem acesso a rede administrativa.
Ameaça 3	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve repor o funcionamento da rede no momento em que o fornecimento de energia for reposto.
Ameaça 4	Identificar a gravidade de incêndio e tomar uma decisão de acordo com essa gravidade: • Foco de incêndio pequeno: apagar o fogo utilizando extintores adequados. Esta ação deve ser realizada apenas por funcionários, que saibam utilizar corretamente os extintores; • Foco de incêndio grande: acionar o corpo de bombeiros da unidade mais próxima (unidade do corpo de bombeiros de Quixeramobim). Esta ação pode ser realizada por qualquer funcionário. Depois do fogo apagado e o prédio liberado para o uso (no caso de incêndio grande, pode haver a necessidade de uma inspeção de segurança do prédio a fim de verificar a integridade do mesmo), o responsável pelo setor de Tecnologia da Informação do campus da universidade deve repor o funcionamento da rede.

Tabela 11 – Execução de cada procedimento

Ordem	Forma de realizar os procedimentos
Ameaça 1	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • Verificar comportamentos anômalos de acordo com padrões pré-estabelecidos (usuários e tráfego da rede); • A partir da análise realizada, identificar de qual porta (rede cabeada) ou de qual Access Point (rede wireless) o acesso foi realizado; • Procurar realizar de alguma forma o bloqueio do dispositivo que acessou irregularmente a rede administrativa; • Trocar a senha de autenticação da rede já que com a senha atual o acesso se encontra disponível para o atacante, entretanto, a troca dessa senha deve ser comunicada a todos os interessados antecipadamente; **Sugestões:** • Adoção de métodos de autenticação mais eficazes, como por exemplo, sistema de autenticação baseada em diretórios (LDAP, Active Directory, outros); • Criação de uma política de senhas que defina responsabilidades, ações e prazos para troca das senhas.
Ameaça 2	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • Identificar o dispositivo que está sendo atacado; • Remover o dispositivo atacado da rede; • Restaurar as configurações do dispositivo a partir do arquivo de configurações backup; • Alterar a senha de acesso ao dispositivo; • Salvar as configurações, inclusive uma versão para backup. **Sugestões:** • Criar senhas únicas para cada dispositivo; • Definir política de troca de senhas dos dispositivos; • Aumentar a segurança da forma que as senhas são armazenadas e compartilhadas entre os responsáveis da rede.

Ameaça 3	O responsável pelo setor de Tecnologia da Informação do campus da universidade deve seguir as seguintes medidas: • No instante em que o fornecimento de energia for reposto, verificar através do software Nagios, os serviços e switchs que voltaram a funcionar e principalmente os que não voltaram a funcionar, para correção do problema; • Verificar quais os Access Points que voltaram a funcionar e principalmente os que não voltaram a funcionar, para correção o problema; • Caso seja necessário realizar a troca de algum dispositivo será necessário realizar a importação de configurações para o dispositivo backup; • Instalar o novo dispositivo no local do outro; • Ligar o novo dispositivo na rede; • Realizar testes de conectividade para verificar a funcionalidade do equipamento. **Sugestão:** configurar uma rede mínima de contingência com pelos menos o firewall e um Access Point ligados aos nobreaks que permita a continuidade do acesso à internet em condições críticas.
Ameaça 4	• Se um funcionário identificar algum foco de incêndio pequeno, ele mesmo deve tentar apaga-lo utilizando-se do extintor ou mangueira de incêndio. Se a pessoa que identificou o foco de incêndio não possuir treinamento, esta deve comunicar o problema rapidamente para alguém que possua tal treinamento; • A partir do momento em que o foco de incêndio estiver controlado, o responsável pela rede deve repor o funcionamento da rede (caso tenha ocorrido alguma falha devido ao incidente) com os dispositivos disponíveis, utilizando-se se necessário dos dispositivos backup e realizar um levantamento das possíveis perdas do ambiente computacional; • Se o incêndio tomar grandes proporções, deve-se acionar o corpo de bombeiros da cidade mais próxima (já que a cidade onde o campus está instalado não possui corpo de bombeiros). Qualquer funcionário pode realizar esta tarefa.

- **Preencha a *Tabela 6 – Melhor Eficiência de Custos, Tabela 7 – Fatores para definição de ameaças/riscos que serão* tratados e *Tabela 9 – Tempo máximo para recuperação da falha*, levando em consideração as seguintes tabelas:**
  - **Tabela 4– Relação de Ameaças/Riscos existentes;**
  - **Tabela 10 – Procedimentos adotados para cada ameaça;**

- **Tabela 11 – Execução de cada procedimento.**

Tabela 6 – Melhor Eficiência de Custos

Ordem	**Custo x benefício (péssimo, ruim, bom, ótimo, excelente)**
Ameaça 1	Excelente
Ameaça 2	Excelente
Ameaça 3	Bom
Ameaça 4	Ruim

Tabela 7 – Fatores para definição de ameaças/riscos que serão tratados

Ordem	**Probabilidade (baixa, média, alta)**	**Consequências do risco (leve, média, grave, gravíssima)**
Ameaça 1	Baixa	Média
Ameaça 2	Baixa	Grave
Ameaça 3	Alta	Leve
Ameaça 4	Baixíssima	Gravíssima

Tabela 9 – Tempo máximo para recuperação da falha

Ordem	**Tempo máximo para recuperação da falha (categoria 1, categoria 2, categoria 3, categoria 4, categoria 5)**
Ameaça1	Categoria 2
Ameaça2	Categoria 2
Ameaça 3	Categoria 2
Ameaça 4	Incêndio pequeno: Categoria 1 Incêndio médio: Categoria 3 Incêndio grande: Categoria 4 ou 5

Zarathon Lopes Viana

Técnico. de Laboratório de Informática

APÊNDICE 05 – Métricas

- **Custo x Benefício** (é o custo x benefício de aplicar procedimentos no intuito de evitar ou reparar algum problema):
    - **Péssimo:** quando o custo para solucionar um problema á alto e seu benefício é pequeno;
    - **Ruim:** quando o custo para solucionar um problema é médio ou alto e seu benefício é pequeno ou médio, respectivamente;
    - **Bom:** quando o custo para solucionar um problema é pequeno, médio ou alto e seu benefício é pequeno, médio ou alto, respectivamente;
    - **Ótimo:** quando o custo para solucionar um problema é pequeno ou médio e seu benefício é médio ou alto, respectivamente;
    - **Excelente:** quando o custo para solucionar um problema é pequeno e seu benefício é alto.

Custo	Benefício	Resultado
Pequeno	Pequeno	Bom
Pequeno	Médio	Ótimo
Pequeno	Alto	Excelente
Médio	Pequeno	Ruim
Médio	Médio	Bom
Médio	Alto	Ótimo
Alto	Pequeno	Péssimo
Alto	Médio	Ruim
Alto	Alto	Bom

- **Probabilidade**:

  A seguinte tabela foi criada para auxiliar nas métricas de probabilidade.

Probabilidade	Valor mensal
Baixa	Eventos com ocorrência anual
Média	Eventos com ocorrência mensal
Alta	Eventos com ocorrência semanal

- **Consequências do risco**:
    - **Leve:** o impacto causado pela falha não irá provocar grandes perdas ou prejuízos. Exemplo: disponibilidade corrompida, confidencialidade e integridade (física e dados) não corrompidas;
    - **Média:** o impacto causado pela falha irá provocar perdas ou prejuízos. Exemplo: disponibilidade e confidencialidade corrompidas, integridade (física e dados) não corrompida;
    - **Grave:** o impacto causado pela falha irá provocar grandes perdas ou prejuízos. Exemplo: disponibilidade, confidencialidade, integridade (dados) são corrompidas e integridade física não corrompida;
    - **Gravíssima:** o impacto causado pela falha irá provocar perdas ou prejuízos catastróficos. Exemplo: disponibilidade, confidencialidade, integridade (física e dados) são corrompidas.

	Disponibilidade	**Confidencialidade**	**Integridade dos dados**	**Integridade Física**
Leve	X			
Média	X	X		
Grave	X	X	X	
Gravíssima	X	X	X	X

- **Tempo máximo para recuperação da falha:**

Categoria	**Tempo máximo para recuperação da falha**
Categoria 1	Até 1 hora
Categoria 2	Até 1 dia
Categoria 3	Até 1 semana
Categoria 4	Até 1 mês
Categoria 5	Acima de 1 mês

ANEXO 1 – POLÍTICA DE SEGURANÇA DA UFC

Classificação	Código	Revisão	Emissão	Folha
☐ C ☐ R ☒ P	P01/STI/UFC	02	10/11/2011	1/7

(C)onfidencial; (R)estrita; (P)ública

Universidade Federal do Ceará
Secretaria de Tecnologia da Informação

Política de Segurança da Informação e Comunicação

ORIGEM

Secretaria de Tecnologia da Informação

REFERENCIA NORMATIVA

Decreto 3505 de 13 de junho de 2000.
Decreto 4553 de 27 de dezembro de 2002.
Normativa Complementar 01/DSIC/GSIPR de 13 de outubro de 2008.
Normativa Complementar 03/DSIC/GSIPR de 30 de junho de 2009.
Normativa Complementar 04/DSIC/GSIPR de 14 de agosto de 2009.
Normativa Complementar 05/DSIC/GSIPR de 14 de agosto de 2009.
Normativa Complementar 06/DSIC/GSIPR de 11 de novembro de 2009.
Normativa Complementar 07/DSIC/GSIPR de 06 de maio de 2010.
Normativa Complementar 08/DSIC/GSIPR de 19 de agosto de 2010.
NBR ISO/IEC 27002:2005.
NBR ISO/IEC 27005:2008.

CAMPO DE APLICAÇÃO

Esta Política se aplica no âmbito da Universidade Federal do Ceará

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

_____
JESUALDO PEREIRA FARIAS
Reitor

1. Escopo

Fazem parte do escopo desta política:

a) Definir diretrizes que orientarão a criação de normas e procedimentos relacionadas à segurança da informação e comunicação no âmbito desta instituição;

b) Apresentar de forma clara a visão desta instituição e de sua administração superior relacionada à segurança da informação e comunicação; e

c) Prover meios para atingir a excelência na qualidade dos serviços prestados por esta instituição, no que tange à confidencialidade, integridade e disponibilidade das informações.

2. Conceitos e Definições

Para efeito desta política, serão adotadas as seguintes definições:

a) Ativo: qualquer bem, material ou não, que tenha valor para esta instituição;

b) Ativo Custodiado: Ativo de terceiro que é administrado e conservado por esta instituição;

c) Ativo de Informação: Ativo que guarda informação de valor para esta instituição;

d) Autenticidade: garantia da veracidade da identidade dos usuários e da origem das informações;

e) Classificação do Ativo: definição do nível de segurança adequado para um Ativo;

f) Confidencialidade: garantia de que uma informação estará disponível apenas para os usuários devidamente autorizados;

g) Cópia de Segurança: cópia reserva que deve ser utilizada no processo de restauração caso a cópia original seja perdida ou danificada. Também conhecida como Backup.

h) Diretriz: conjunto de orientações que devem ser observadas para a produção de Normas e Procedimentos específicos;

i) Disponibilidade: garantia de que uma informação estará disponível sempre que os usuários autorizados necessitarem;

j) Gestor do Ativo: membro desta instituição responsável pela segurança de um determinado Ativo;

k) Incidente de Segurança: evento identificado em um Ativo que indica uma violação da Política de Segurança da Informação e Comunicação;

l) Integridade: garantia de que uma informação estará disponível de forma correta e completa, sem adulterações;

m) Norma: conjunto de regras que devem ser seguidas por um grupo;

n) Política de Segurança da Informação e Comunicação: conjunto de princípios que norteiam a gestão da segurança da informação e que devem ser observados pelo corpo técnico e gerencial da instituição, bem como por seus usuários internos e externos, a fim de garantir

que os Ativos sejam assegurados; e

o) Procedimento: conjunto de ações que devem ser realizadas por um grupo para produzir algo.

3. Princípios

Esta política tem como fundamento os seguintes princípios:

a) Confidencialidade: deve ser garantido que apenas os usuários autorizadas tenham acesso aos Ativos;

b) Integridade: deve ser garantido que os Ativos sejam mantidos corretos e completos;

c) Disponibilidade: deve ser garantido que os usuários autorizados tenham acesso aos Ativos sempre que necessário; e

d) Autenticidade: deve ser garantido que os usuários sejam quem eles dizem ser e que as informações sejam realmente provenientes das origens indicadas.

4. Diretrizes Gerais

Esta política e seus documentos complementares são regidos pelas Diretrizes apresentadas a seguir. Elas devem orientar a definição de Normas e Procedimentos específicos relacionados com a segurança da informação e comunicação.

4.1. Tratamento dos Ativos

Com relação ao Tratamento dos Ativos, que envolve a Identificação, Classificação, Manipulação e Conservação dos Ativos, devem ser considerados os seguintes aspectos:

a) todo Ativo Custodiado ou de propriedade desta instituição deve ser inventariado;

b) todo Ativo de Informação produzida por membros desta instituição, no exercício de suas atividades, é de propriedade desta instituição;

c) todo Ativo Custodiado ou de propriedade desta instituição deve ser protegido segundo as Diretrizes descritas nesta política e nas demais regulamentações em vigor;

d) todo Ativo Custodiado ou de propriedade desta instituição deve ter um Gestor do Ativo, sobre quem recai a responsabilidade sobre a segurança do respectivo Ativo;

e) todo Ativo de Informação custodiado ou de propriedade desta instituição deve ser classificado quanto aos aspectos de confidencialidade, integridade e disponibilidade, de forma explícita ou implícita. Esse processo de classificação deve ser implementado e mantido, em conformidade com a legislação vigente, visando estabelecer os controles de segurança necessários a cada Ativo de Informação;

f) todo Ativo Custodiado ou de propriedade desta instituição deve ser cedido somente mediante autorização formal. Essa autorização deve observar a classificação da informação e a legislação vigente; e

g) toda classificação e cessão dos Ativos deve ser feita pelo respectivo Gestor do Ativo.

4.2. Controle de Acesso

Com relação ao Controle de Acesso, que envolve o Acesso Lógico e Físico aos Ativos, devem ser considerados os seguintes aspectos:

a) todo uso dos Ativos deve ser autorizado pelo respectivo Gestor do Ativo e ocorrer mediante identificação única e intransferível do usuário;

b) todo uso dos Ativos deve ser controlado e limitado ao mínimo necessário para o cumprimento das atividades de cada usuário. Qualquer outra forma de uso deve ser previamente autorizada formalmente pelo respectivo Gestor do Ativo;

c) sempre que houver a admissão, mudança das atribuições ou desligamento dos usuários será responsabilidade da chefia imediata solicitar dos Gestores dos Ativos utilizados providências imediatas para os ajustes necessários dos privilégios de acesso dos respectivos Ativos; e

d) todo ambiente deve ser classificado e protegido com mecanismos adequados de segurança de acordo com a criticidade e o sigilo dos Ativos que são mantidos naquele local.

4.3. Auditoria e Conformidade

Com relação à Auditoria e Conformidade devem ser considerados os seguintes aspectos:

a) todo uso de Ativo, sempre que possível, deve gerar trilhas de auditoria que devem ser mantidos para efeito de análise segundo as diretrizes descritas nesta política e as demais regulamentações em vigor;

b) todo uso de Ativo é passível de monitoramento e auditoria, e sempre que possível deve ser analisado em busca de indícios de descumprimento desta política; e

c) deve ser estabelecido procedimento formal para notificação de casos de violação das regras definidas pelo conjunto de documentos que compõem esta política.

4.4. Gestão de Continuidade

Com relação à Gestão de Continuidade, que envolve o Backup, Plano de Contingência, Testes, Treinamentos e Documentação de procedimentos, devem ser considerados os seguintes aspectos:

a) deve ser estabelecida a gestão de continuidade no âmbito desta instituição com o objetivo de minimizar os impactos de falhas fortuitas dos Ativos que suportam as operações desta instituição;

b) deve ser elaborado plano de contingência para o restabelecimento das operações críticas interrompidas por falhas fortuitas dos Ativos desta instituição;

c) todo Ativo de Informação desta instituição, seja eletrônico ou não, deve ser armazenado em meio que ofereça salvaguarda adequada e segurança;

d) todo Ativo de informação desta instituição, se eletrônico, deve dispor de Cópia de Segurança atualizada regularmente e com frequência adequada; e

e) toda Cópia de Segurança deve ser mantida em lugar seguro e diferente do lugar onde o respectivo Ativo de Informação está localizado. O lugar escolhido deve garantir a segurança da cópia caso alguma ameaça a que está sujeito o respectivo Ativo de Informação se concretize.

4.5. Gestão de Risco

Com relação à Gestão de Risco, que envolve o Inventariamento dos Ativos, Análise, Avaliação, Tratamento, Aceitação, Comunicação e Monitoramento dos Riscos, devem ser considerados os seguintes aspectos:

a) todo impacto associado aos Ativos deve ser avaliado e, se possível, minimizado; e

b) toda ação de segurança da informação deve ser feita com base na avaliação da criticidade dos Ativos.

5. Competências e Responsabilidades

Para o efetivo cumprimento das diretrizes estabelecidas por esta política, ficam instituídas as seguintes competências e responsabilidades nesta instituição:

5.1. Autoridade Máxima

São responsabilidades da Autoridade Máxima desta instituição:

a) instituir o Comitê Gestor de Segurança da Informação e Comunicação;

b) instituir o Gestor de Segurança da Informação e Comunicação;

c) instituir o Departamento de Segurança da Informação e Comunicação;

d) aprovar a Política de Segurança da Informação e Comunicação; e

e) garantir os recursos necessários para implementação destas diretrizes.

5.2. Comitê Gestor de Segurança da Informação e Comunicação

São responsabilidades do Comitê Gestor de Segurança da Informação e Comunicação desta instituição:

a) analisar e aprovar normas, procedimentos e soluções específicas que atendam às necessidades de segurança da informação e comunicação;

b) apoiar a implementação das ações de segurança da informação e comunicação; e

c) analisar os casos relacionados à segurança da informação e comunicação omissos nesta política.

5.3. Gestor de Segurança da Informação e Comunicação

São responsabilidades do Gestor de Segurança da Informação e Comunicação desta instituição:

a) assessorar e contribuir com as atividades do Comitê Gestor de Segurança da Informação e Comunicação;

b) coordenar e contribuir com as atividades do Departamento de Segurança da Informação e Comunicação;

c) promover a cultura institucional de Segurança da Informação e Comunicação;

d) propor recursos necessários às ações de Segurança da Informação e Comunicação; e

e) representar a instituição para tratar de assunto relacionados a Segurança da Informação e Comunicação.

5.4. Departamento de Segurança da Informação e Comunicação

São responsabilidades do Departamento de Segurança da Informação e Comunicação desta instituição:

a) capacitar e conscientizar os membros desta instituição sobre Segurança da Informação e Comunicação;

b) desenvolver atividades relacionadas a Gestão de Risco, conforme previsto nesta política;

c) desenvolver atividades relacionadas a Auditoria e Conformidade, conforme previsto nesta política.

d) monitorar, sempre que possível, os Ativos de forma a identificar a ocorrência de Incidentes de Segurança; e

e) tratar e responder os Incidentes de Segurança identificados ou reportados.

5.5. Membros

São responsabilidades dos Membros desta instituição:

a) estar ciente e seguir esta política e as demais regulamentações em vigor relacionadas a segurança da informação; e

b) comunicar formalmente ao Grupo de Tratamento e Resposta a Incidentes, por meio de processo formal, qualquer incidente de segurança, suspeito ou confirmado, que venha a tomar conhecimento e possa comprometer a segurança de ativos desta instituição.

6. Penalidades

A violação desta política e dos instrumentos normativos gerados a partir dela resultarão em penas e sansões legais impostas por processos administrativos, conforme previsto pelo regimento interno desta instituição, sem prejuízo das demais medidas cíveis e penais cabíveis.

7. Atualização

Esta política e os instrumentos normativos gerados a partir dela devem ser revisados sempre que necessário, contanto que não exceda o período máximo de 1 (um) ano.

8. Histórico de Mudanças

Na Tabela 1 devem ser registradas todas as alterações realizadas nesta política.

Data	Revisão	Responsável	Detalhes
19/07/2011	00	Márcio Correia	Produção da versão inicial para aprovação
22/07/2011	01	Márcio Correia	Realizados ajustes aprovados na reunião do comitê dirigente da STI. Basicamente questões relacionadas com a redação do documento.
10/11/2011	02	Márcio Correia	Realizados ajustes aprovados na reunião com os Diretores Geral e Adjunto da STI. Correções ortográficas. Ajustes nos conceitos e definições utilizados. Realizadas também melhorias no detalhamento e adequação das Competências e Responsabilidades.

Tabela 1 – Tabela de histórico de mudanças desta política.