



**XXI SNPTTE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA**

Versão 1.0
23 a 26 de Outubro de 2011
Florianópolis - SC

GRUPO - XV

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS - GTL

CONTINUIDADE DE NEGÓCIOS APLICADA A TECNOLOGIA DA INFORMAÇÃO E TELECOMUNICAÇÕES

**Ricardo Roscoe
ELETROBRAS ELETRONORTE**

RESUMO

A presente instrução técnica tem como objetivo descrever as recomendações de governança de tecnologia de informação no que diz respeito à Gestão de Continuidade de Negócios. Sob a ótica da governança institucional, também serão tratadas as consequências da abertura do capital acionário da Eletrobrás na Bolsa de Valores de Nova Iorque, que tornou obrigatório a adequação dos processos e controles internos associados aos relatórios financeiros das empresas do Sistema Eletrobrás às determinações da Lei Sarbanes-Oxley, também chamada de SOX. Além disto, serão discutidos os resultados atingidos pelo grupo de trabalho da Eletrobras Eletronorte responsável pelo estudo do Centro de Contingência da Eletronorte que tem como diretriz principal a recomposição dos sistemas de missão crítica (TI, telecomunicações e operação).

PALAVRAS-CHAVE

Gestão de continuidade de negócio, NBR 15999, ITIL, COBIT, Lei Sarbanes-Oxley (SOX).

1.0 - INTRODUÇÃO

Os sistemas e serviços de Tecnologia da Informação e Telecomunicações são essenciais para as empresas do Setor de Energia Elétrica as quais possuem função estratégica para o desenvolvimento e manutenção da soberania brasileira. Os sistemas corporativos das empresas que dão suporte aos processos de gestão, operação e manutenção devem estar sempre disponíveis em tempo real e com confiabilidade, uma vez que eles são os pilares para a tomada de decisões estratégicas.

Os sistemas de Tecnologia da Informação e Telecomunicações estão susceptíveis a uma variedade imensa de ameaças que podem ocasionar a perda parcial ou total dos serviços que deles dependem. Estas ameaças podem ser classificadas de acordo com sua natureza: Natural (enchentes, incêndios, tornados, etc); Humana (erros humanos, sabotagem, ataques terroristas, guerras, etc); Infraestrutura (falhas de equipamentos, erros de software, falhas de alimentação, indisponibilidade de meios de telecomunicações, etc). Diante disto, é fundamental que as empresas do grupo Eletrobrás desenvolvam a Gestão de Continuidade do Negócio (GCN) com o intuito de não permitir a interrupção das atividades operacionais e de gestão, garantindo as condições mínimas necessárias para o retorno rápido e seguro dos sistemas de missão crítica das empresas.

A Gestão de Continuidade de Negócios (GCN) estabelece as diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a capacidade estratégica de uma organização no sentido de planejar e responder a incidentes e interrupções de negócios, para conseguir continuar suas operações em um nível aceitável previamente definido.

2.0 - MODELOS DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS E GOVERNANÇA DE TI

2.1 Control Objectives for Information and Related Technology - COBIT

O COBIT (Control Objectives for Information and Related Technology) foi criado em 1994 pela ISACF (Information Systems Audit and Control Foundation), a partir de seu conjunto inicial de controles, e vem evoluindo através da incorporação de padrões específicos para processos de TI. O principal objetivo do COBIT é contribuir para a entrega de serviços e produtos de TI, a partir da perspectiva das necessidades do negócio, através de uma abordagem com foco mais acentuado no controle do que na execução.

A estrutura do COBIT foi concebida para atender as necessidades de controle da organização relacionadas à Governança de TI, tendo como principais características o foco nos requisitos de negócio, a orientação para uma abordagem de processos, a utilização extensiva de mecanismos de controle e o direcionamento para a análise das medições e indicadores de desempenho.

Utilizando o modelo PDCA (Plan-Do-Check-Act) de melhoria contínua o COBIT define 34 processos de TI distribuídos em quatro domínios mostrados a seguir:

- a. Planejamento e Organização: Identifica como a TI pode contribuir para o atendimento dos objetivos de negócios da organização, envolvendo planejamento, comunicação e gerenciamento;
- b. Aquisição e Implantação: Identificação, manutenção, desenvolvimento e/ou aquisição de soluções de TI de acordo com a estratégia estabelecida pela organização bem como a sua integração junto aos processos de negócio;
- c. Entrega e Suporte: Entrega dos serviços requeridos, incluindo gerenciamento de segurança, continuidade dos serviços, suporte aos serviços para usuários, gestão de dados e infraestrutura operacional;
- d. Monitoração e Avaliação: Assegura a qualidade dos processos de TI por meio de rotinas de acompanhamento, monitoração e de avaliações.

A metodologia do COBIT é voltada para três níveis distintos: para gerentes que necessitam avaliar os riscos e controlar os investimentos de TI; para os usuários que precisam assegurar a qualidade dos serviços prestados para clientes internos e externos; e para auditores que necessitam avaliar o trabalho de gestão da TI e aconselhar o controle interno da organização.

2.2 Information Technology Infrastructure Library – ITIL

A ITIL (Information Technology Infrastructure Library) foi desenvolvida no final dos anos 80 pelo CCTA (Central Computer and Telecommunications Agency) com o objetivo de desenvolver melhores práticas para o gerenciamento de serviços de TI objetivando o alinhamento e integração com as necessidades dos clientes e usuários destes serviços. Os processos da ITIL encontram-se distribuídos entre 5 (cinco) estágios do ciclo de vida do serviço de TI:

- a. Estratégia do Serviço: Orienta sobre como as políticas e processos de gerenciamento de serviço podem ser desenhados, desenvolvidos e implementados;
- b. Desenho do Serviço: Orienta para estruturação e desenvolvimento dos serviços e dos processos de gerenciamento de serviços;
- c. Transição de Serviço: Orienta sobre como efetivar a transição de serviços novos para operações já implantadas;
- d. Operação de Serviço: Descreve a fase de ciclo de vida do gerenciamento de serviços que é responsável pelas atividades rotineiras;
- e. Melhoria de Serviço Continuada: Orienta sobre como fazer sistematicamente melhorias incrementais e de larga escala na qualidade dos serviços.

O processo de Gerenciamento da Continuidade de Serviço, integrante do estágio de Desenho do Serviço, é um desdobramento do processo de gerenciamento da continuidade de negócios, que visa assegurar que todos os recursos técnicos e recursos de TI necessários (incluindo sistemas, telecomunicações, redes, aplicações, etc.) possam ser recuperados dentro de um tempo preestabelecido.

2.3 NBR 15999 – Gestão de Continuidade de Negócios

A associação Brasileira de Normas Técnicas (ABNT) desenvolveu, por meio de especialistas da comunidade de continuidade de negócios, a NBR 15999 sob o título geral de “Gestão de continuidade de negócios” e composta pelas seguintes partes: Parte 1 – Código de prática (NBR 15999-1) e Parte 2 – Requisitos (NBR 15999-2).

A NBR 15999-1 estabelece o processo, os princípios e a terminologia da gestão de continuidade de negócios. Ela foi elaborada como um código de práticas que visa fornecer uma base para que se possa entender, desenvolver, implementar e manter a continuidade de negócios em uma organização.

Segundo a NBR 15999-1, a gestão de continuidade de negócios é o processo que identifica as ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo de gestão fornece uma estrutura para que se desenvolva uma resiliência da organização contra possíveis interrupções de sua capacidade de atingir seus principais objetivos e que seja capaz de responder efetivamente e salvaguardar os interesses, a reputação, a marca da organização e suas atividades de valor agregado.

A gestão de continuidade de negócios envolve o gerenciamento da recuperação ou da continuidade das atividades no caso de uma interrupção de negócios e o gerenciamento do programa de continuidade por meio de treinamentos, testes e análises críticas, de forma a garantir que os planos de continuidade de negócios estejam sempre atualizados.

Segundo a NBR 15999-1 a gestão da continuidade de negócio é estruturada em seis elementos obrigatórios, que compõem o ciclo de vida da GCN, que podem ser implementados em organizações de diversos setores e tamanhos.



FIGURA 1 – Mapa mental do Ciclo de vida GCN segundo a NBR 15999-1

A NBR 15999-2 adota o modelo PDCA (Plan-Do-Check-Act) de melhoria contínua para estabelecer, implementar, operar, monitorar, treinar, manter e melhorar a eficácia do Sistema de Gestão de Continuidade de Negócio (SGCN) definido por um programa de GCN de uma organização.

3.0 - LEI SARBANES-OXLEY (SARBANES-OXLEY ACT)

A Lei Sarbanes-Oxley, mais conhecida como SOX ou SOA, foi publicada em 2002 a partir da necessidade de proteção dos investidores americanos contra fraudes contábeis e financeiras de empresas de capital aberto, restabelecendo e aumentando a confiança do investidor e a sustentabilidade das organizações.

Em suas diversas seções a SOX possui 2 (duas) que são de suma importância para TI. A seção 302 trata da responsabilidade corporativa pelos relatórios financeiros, o que requer um comprometimento dos diretores (executivos e financeiros) na acuracidade dos relatórios financeiros. A seção 404 trata da avaliação do gerenciamento dos controles internos, o que requer que os diretores (executivos e financeiros) e auditores externos confirmem a eficácia e a acuracidade dos controles internos para os relatórios financeiros. A tabela a seguir mostra as principais aplicações operacionais do SOX para TI.

Tabela 1: Implicação da SOX para TI.

REQUISITOS DE QUALIDADE DA INFORMAÇÃO	IMPLICAÇÕES DO SOX
O conteúdo da informação deve ser apropriado.	<ul style="list-style-type: none"> • Processo de desenvolvimento de requisitos de software; • Processo de gerenciamento de requisitos de software; • Métodos de engenharia de software; • Processos de verificação (teste); • Processos de validação (aceitação pelos usuários); • Processos de segurança da informação empregados nos aplicativos; • Processos de aceitação de produtos de terceiros; • Processo de gestão da mudança e da configuração.
A informação deve estar disponível no momento em que for necessária.	<ul style="list-style-type: none"> • Disponibilidade de aplicativos; • Disponibilidade de infraestrutura; • Gerenciamento de incidentes e problemas no ambiente de produção; • Suporte aos usuários; • Gestão de aplicativos e de ativos de TI; • Processos de gerenciamento da infraestrutura; • Segurança da infraestrutura; • Gerenciamento da contingência; • Gerenciamento de disponibilidade e desempenho.
A informação é atual ou pelo menos é a última disponível.	<ul style="list-style-type: none"> • Processo de gerenciamento de dados; • Planejamento e gerenciamento da contingência e de desastres; • Segurança da informação na infraestrutura.
Os dados e as informações estão corretos.	<ul style="list-style-type: none"> • Segurança da informação em aplicativos; • Segurança da infraestrutura de TI; • Teste de software; • Controle da mudança e da configuração; • Gerenciamento de dados; • Gerenciamento de requisitos.
A informação é acessível aos interessados.	<ul style="list-style-type: none"> • Segurança da informação referente a controle de acessos e privilégios; • Controle de autorizações;
Há um sistema de controle interno sobre relatórios financeiros.	<ul style="list-style-type: none"> • Avaliação de riscos de TI; • Gestão da qualidade; • Planos de desastre e recuperação.

4.0 - ANÁLISE DE IMPACTO DE NEGÓCIO

A Análise de Impacto de Negócio (BIA – Business Impact Analysis) é peça fundamental no processo de gerenciamento de continuidade de negócios e dos planos de contingência de uma organização. Ela envolve a avaliação e priorização das funções e processos do negócio que devem ser recuperados. A organização deverá executar a caracterização completa dos requisitos de sistema, processos e suas interdependências, e usar esta informação para determinar os requisitos de contingência e suas prioridades.

O propósito da Análise de Impacto de Negócio é correlacionar componentes de sistemas específicos com os serviços críticos que são providos por eles, e baseando-se nestas informações, caracterizar as consequências quando da interrupção destes. A organização deverá estimar o tempo máximo de interrupção permitido e o nível aceitável de perdas (dados, operacionais, financeiras, reputação, etc) associadas ao tempo de interrupção. Os resultados desta etapa irão subsidiar o estabelecimento do tempo objetivado de recuperação (RTO – Recovery Time Objective) e a recuperação dos processos ou sistemas estratégicos que irão receber maior prioridade durante a recuperação. Além disto, a organização deverá determinar o ponto ideal de recuperação dos processos identificados (TI, telecomunicações, operação, etc) através do balanceamento do custo associado à interrupção versus o custo dos recursos necessários de restauração.

5.0 - GESTÃO DE RISCO

A gestão de risco consiste no processo de identificação, avaliação e mitigação do risco a um nível aceitável de forma a manter os processos críticos de uma organização. A avaliação do risco é obtida através das análises de processos, ativos físicos, tecnológicos e humanos orientados para as melhores práticas através da construção do relacionamento entre processos, sistemas/serviços e ativos.

A definição de uma estratégia de mitigação de risco pela organização é peça fundamental para o sucesso da gestão de risco e da continuidade de negócios. Várias alternativas devem ser consideradas na definição da estratégia de uma organização, incluindo o custo, tempo de interrupção permitido, segurança e outros requisitos estratégicos para a organização. A estratégia de mitigação de risco escolhida deve conter uma combinação de métodos que se complementam e fornecem uma vasta capacidade de recuperação a partir de diversos tipos de incidentes.

A seguir serão discutidos alguns métodos que devem ser considerados na estratégia de mitigação de risco de uma organização.

a. Site Alternativo

É uma instalação alternativa na qual os serviços essenciais, definidos na Análise de Impacto de Negócio, são recuperados após um incidente que comprometa o site principal de uma organização. O site alternativo pode ser categorizado de acordo com a disponibilidade operacional que ele irá proporcionar:

- Cold-site: Consiste em um ambiente com os recursos mínimos de infraestrutura. Este site não contém equipamentos de TI, telecomunicações e de escritório (telefones, desktop, fax, etc);
- Warm-site: Consiste em um ambiente parcialmente ou totalmente equipado com sistemas de hardware, software, telecomunicações e infraestrutura. Neste site os sistemas críticos estão disponíveis para realocação imediata, porém talvez seja necessária a preparação antes de receber os sistemas e a equipe de contingência;
- Hot-site: Consiste em um ambiente totalmente equipado com sistemas de hardware, software, telecomunicações, infraestrutura e equipe de suporte. Neste site os sistemas críticos estão disponíveis para realocação imediata, e não é necessária nenhuma preparação antes de receber os sistemas e a equipe de contingência;
- Mirrored-Site: Consiste em um ambiente totalmente espelhado com o site principal. Este site é idêntico ao site principal no que diz respeito aos aspectos técnicos. Este site fornece o grau máximo de disponibilidade uma vez que os dados são armazenados e processados no site principal e alternativo simultaneamente.

b. Backup e Armazenamento Offsite

Backup é o processo periódico de TI no qual os dados de produção, aplicação, sistemas e usuário são copiados para uma mídia diferente de armazenamento, estando assim disponíveis no caso de alguma perda indesejada. Os dados podem ser armazenados em discos magnéticos (disk library), fitas (tape library) ou discos ópticos (CD's, DVD's, etc). A utilização de backups em disco (disk library) tem sido muito difundida, uma vez que esta tecnologia é capaz de emular os diversos tipos de fitas (tapes) e, desta forma, permite a sua implantação em uma organização sem a necessidade de modificação na operação e na infraestrutura de backup. Políticas de backup's devem especificar a frequência dos backup's (diária, mensal, semestral, etc) baseado na importância e na frequência que as novas informações são inseridas.

Independentemente do método de armazenamento de backup utilizado por uma organização, é crucial a definição do local de armazenamento das mídias de forma segura. A utilização de um armazenamento offsite destas mídias garante que um incidente no site principal não impeça a continuidade dos negócios de uma organização. O local de armazenamento offsite deve possuir proteção contra emissões eletromagnéticas, incêndio e controle de acesso para pessoas não autorizadas.

c. Failover

Consiste na capacidade de comutação (automática ou manual), em caso de falha, de um sistema principal para seu correspondente reserva. A distância de rede entre os sistemas principal e reserva deve ser cuidadosamente considerada, pois pode ter impacto negativo na operação de TI de uma organização.

A utilização de técnicas de virtualização, tanto de servidores como de storages, em conjunto com NAS (network-attached storage) e SAN (Storage Área Network) permite que o failover seja mais transparente e menos impactante para uma organização.

d. Cluster de Alta Disponibilidade

O cluster de alta disponibilidade, também denominado de “high-availability cluster” ou “failover cluster”, consiste na arquitetura de servidores aonde dois servidores completos são utilizados e a função do segundo servidor é assumir as funções do primeiro em caso de falha deste.

e. Balanceamento de Carga (Load Balance)

O balanceamento de carga (load balance) consiste em uma estrutura de vários servidores ligados em rede de forma a dividir as requisições de carga de forma balanceada. No caso de aplicativos de carga balanceada, quando um servidor falha ou fica offline, a carga é automaticamente redistribuída entre os servidores ainda em operação.

f. Infraestrutura

Em muitos casos os impactos de uma interrupção não planejada podem ser mitigados e/ou eliminados através de implantações de soluções infraestrutura tais como:

- Sistema de detecção de fogo e fumaça;
- Sistema de combate a incêndio;
- Grupo moto gerador (GMG) para o fornecimento de alimentação reserva de longa duração;
- Sistema de No-break e UPS (Uninterruptible Power Supply) para o fornecimento de alimentação reserva de curta duração. Em conjunto com o GMG estes sistemas servem para fornecer alimentação necessária para os sistemas até a partida do GMG;
- Sistemas ar-condicionado redundantes;
- Salas cofre para o armazenamento dos sistemas mais críticos;
- Sistema de aterramento eficiente para evitar interrupções causadas por descargas atmosféricas;
- Controle de acesso para pessoas não autorizadas;
- Rede de dados com links redundantes.

6.0 - PROJETO SOX ELETROBRÁS

Desde 1995 a Eletrobrás negocia seus títulos na Bolsa de Nova Iorque (NYSE) no chamado ADR nível 1. Esta modalidade de negociação, também chamada de mercado de balcão, não exige o registro na SEC – Securities and Exchange Commission (órgão equivalente à CVM – Comissão de Valores Mobiliários).

A partir de 2003 a Eletrobrás vem atuando para comercializar suas ações via Certificados de Depósitos Bancários Norte Americanos (ADR nível 2). Esta iniciativa, que envolve todas as subsidiárias do Sistema Eletrobrás, possui as seguintes vantagens:

- a. Visibilidade: Torna a Eletrobrás atraente para negócios e investidores interessados em constituir parceria com uma empresa sólida e sustentável;
- b. Credibilidade: Dá a empresa uma imagem de confiabilidade no mercado, pois o rigor dos requisitos para a entrada na NYSE é muito alto;
- c. Captação: Facilita a captação de recursos no mercado internacional graças à imagem de empresa confiável adquirida;
- d. Valor: Aumenta o valor de mercado da empresa, pois a reputação que vem com a credibilidade passa a entrar no cálculo do seu valor juntamente com os demais ativos.

Para poder negociar suas ações na ADR nível 2 a Eletrobrás e suas subsidiárias necessitam dos seguintes requisitos: registro na SEC; adaptação da contabilidade aos padrões americanos; e adequação às exigências regulatórias da Lei Sarbanes-Oxley (SOX).

Em 2005 a Eletrobrás iniciou, em conjunto com a consultoria Ernst & Young, o Projeto SOX que tem como objetivo promover a adequação às normas exigidas pela SOX. O Projeto SOX compõe-se das seguintes fases:

- a. Fase 1: Planejamento geral do projeto, compreensão da definição de controle interno, organização da equipe de trabalho para realizar a avaliação do controle interno no nível da entidade;

- b. Fase 2: Compreensão e avaliação dos controles internos em nível de processo, transação ou aplicação;
- c. Fase 3: Avaliação da eficácia de forma geral, identificação de pontos a serem aprimorados e estabelecimento de sistemas de monitoramento e certificação da administração sobre os controles internos.

6.1 Centro de Contingência da Eletrobras Eletronorte

Como consequência da implantação do Projeto SOX e das imposições da Lei Sarbanes Oxley, no que diz respeito à mitigação de riscos associados a eventuais sinistros ou impedimentos de acesso ao edifício Sede da Eletrobras Eletronorte, foi formado, no final de 2008, um grupo de trabalho responsável pela definição do melhor local de instalação do Centro de Contingência. O Centro de Contingência da Eletrobras Eletronorte foi definido tendo em vista as seguintes diretrizes básicas:

- Atendimento às exigências técnicas e às normas pertinentes;
- Otimização tecnológica;
- Menor custo;
- Garantia de recomposição de 100% dos sistemas de missão crítica (TI, Telecomunicações e Operação), no prazo de 8 horas.

Para o estudo do Centro de Contingência o grupo de trabalho efetuou a análise de risco e custo associada aos seguintes cenários:

- a. Cenário 1: Consiste na alocação do site backup (Centro de Contingência) no mesmo prédio do site principal (Sede da Eletrobras Eletronorte) ou bem próximo a ele. Neste cenário os riscos de que um mesmo evento inviabilize os meios de comunicação e a infraestrutura dos sites principal e backup é muito grande, o que causaria um tempo de recuperação muito alto.
- b. Cenário 2: Consiste na alocação do site backup em uma distância entre 10km e 30km do site principal. Neste cenário os sites (principal e backup) estariam distantes o suficiente de forma que um mesmo evento não afetaria os meios de comunicação e infraestrutura. Além disto, a equipe especializada da Sede poderia ser facilmente deslocada para o site backup, o suporte do fornecedor seria o mesmo do prestado ao site principal e os meios de comunicação poderiam ser compartilhados entre os dois sites com um investimento relativamente pequeno. Porém, a desvantagem deste cenário são os custos envolvidos na preparação da infraestrutura necessária para construção do site backup.
- c. Cenário 3: Consiste na alocação do site backup em outra unidade regional da Eletrobras Eletronorte. Neste cenário os sites (principal e backup) estariam distantes o suficiente de forma que um mesmo evento não afetaria os meios de comunicação e infraestrutura. Porém, com este cenário a Eletrobras Eletronorte terá altos riscos e custos associados à logística, suporte dos fornecedores, infraestrutura e comunicação, ocasionando em um alto tempo de recuperação.

As propostas estudadas de acordo com os cenários existentes orientaram o grupo de trabalho para a escolha do Cenário 2 onde seria instalado um Centro de Contingência do tipo Warm-Site.

Com relação a TI, o ambiente a ser contingenciado seria o Centro de Processamento de Dados da Eletrobras Eletronorte. Dentre os sistemas a serem contingenciados vale destacar o software de aplicação empresarial SAP R/3 que possui diversos módulos que dão suporte aos diversos processos da Eletrobras Eletronorte (inclusive o financeiro).

A Eletrobras Eletronorte possui uma rede de telecomunicações composta por um sistema DWDM, com 8 canais de 2,5 GB, que interliga sua Sede ao ONS e ao ponto de acesso com as regionais¹. Para o Centro de Contingência seria feita uma ampliação deste sistema e a implantação de um anel óptico DWDM que seria responsável pela comunicação de voz e dados entre a Sede da Eletrobras Eletronorte, o ONS, o ponto de acesso com as regionais e o Centro de Contingência.

No que diz respeito aos centros de operação e análise, localizados na Sede da Eletrobras Eletronorte, o Centro de Contingência deverá contemplar um espaço para estas áreas e toda infraestrutura de TI e telecomunicações necessárias para a manutenção de seus serviços.

7.0 - CONCLUSÃO

Como pode ser observado neste informe técnico, é de extrema importância que as empresas implantem a Gestão de Continuidade de Negócios em conjunto com técnicas de governança de TI. Desta forma, além de obter a credibilidade no mercado nacional e internacional, elas estarão aptas a superar as ameaças que possam causar

¹ Atualmente o ponto de acesso é responsável pela comunicação da Sede da Eletrobras Eletronorte com as regionais do Tocantins, Maranhão e Pará. Futuramente serão interligadas as regionais do Mato Grosso, Rondônia e Acre.

alguma interrupção inesperada na sua estrutura estratégica.

Vale ressaltar a iniciativa da Eletrobras Eletronorte na construção de uma estrutura sólida para mitigação do risco. Esta estrutura irá contemplar vários níveis de proteção:

- a. Infraestrutura: Esta proteção consistirá na utilização de técnicas e melhores práticas voltadas para a proteção da infraestrutura de TI e telecomunicações da Eletrobras Eletronorte. Dentre as diversas técnicas deve-se destacar: telecomunicações; alimentação; controle de acesso; e equipamentos.
- b. Dados: Esta proteção consistirá na utilização de técnicas e melhores práticas voltadas para a proteção dos dados da Eletrobras Eletronorte. Dentre as diversas técnicas deve-se destacar: backup; armazenamento offsite; e replicação de dados;
- c. Aplicação: Esta proteção consistirá na utilização de técnicas e melhores práticas voltadas para a proteção das aplicações (principalmente o SAP) da Eletrobras Eletronorte. Dentre as diversas técnicas deve-se destacar: balanceamento de carga (load balance); sistemas redundantes; failover; e clusters;
- d. Site: Esta proteção consistirá na utilização de técnicas e melhores práticas voltadas para a proteção do site da Eletrobras Eletronorte. Dentre as diversas técnicas deve-se destacar o Centro de Contingência.

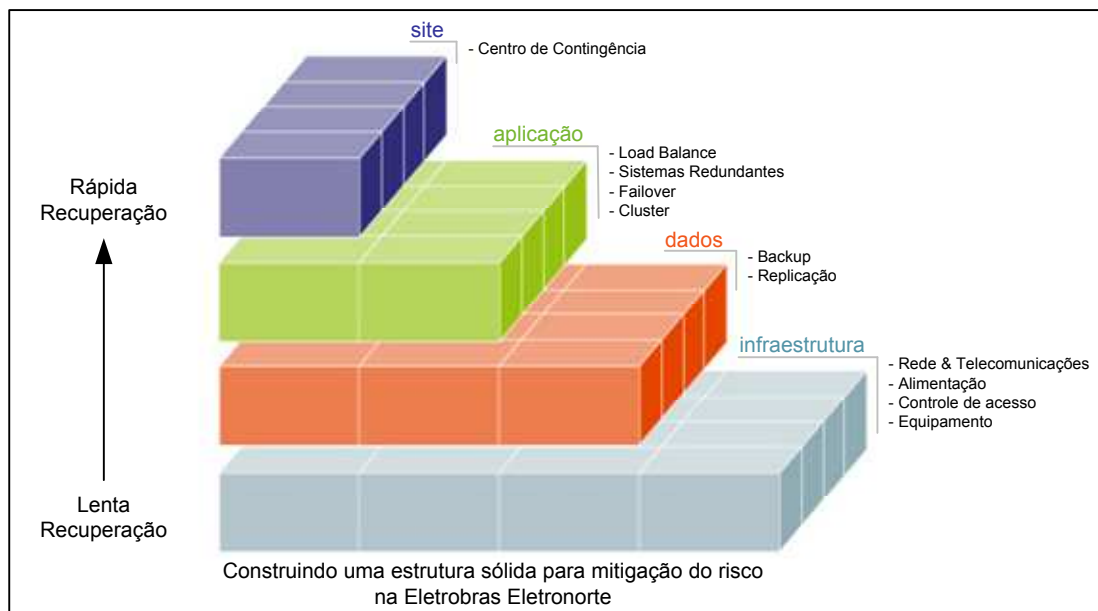


FIGURA 3 – Estrutura de mitigação de risco em implantação na Eletrobras Eletronorte.

Ao optar por um Centro de Contingência tipo Warm-site a Eletrobras Eletronorte estará consolidando as diversas técnicas de mitigação de risco e estará garantindo a rápida recuperação de seus sistemas críticos (TI, Telecomunicações e Operação).

8.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) FERNANDES, A.F. & ABREU V.F. Implantando a Governança de TI: da estratégia à gestão dos processos e serviços - 2ª Edição – Editora Brasport. Brasil, 2008;
- (2) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Especial Publication 800-34: Contingency Planning Guide for Information Technology Systems. Estados Unidos da América, 2002;
- (3) ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de continuidade de negócios Parte 1: Código de prática - NBR 15999-1. Brasil, 2007;
- (4) ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Gestão de continuidade de negócios Parte 2: Requisitos - NBR 15999-2. Brasil, 2008;
- (5) ELETROBRAS ELETRONORTE. Relatório do Grupo de Trabalho Constituído pela Resolução de Diretoria – RD 888/2008. Brasil, 2009.
- (6) FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUCL. Business Continuity Planning – IT Examination Handbook. 2008.

9.0 - DADOS BIOGRÁFICOS

Ricardo Roscoe

Nascido em Brasília-DF em 10 de junho de 1975.

Graduado (2003) em Engenharia de Redes de Comunicações pela Universidade de Brasília - UnB

Empresa: Eletrobras Eletronorte, desde 2008.

Atua na Gerência de Redes de Telecomunicações – CETR