

MOISES THIEME

**MODELO DE GOVERNANÇA EM FACILIDADES PREDIAIS
PARA CENTROS DE TECNOLOGIA DA INFORMAÇÃO
DE INSTITUIÇÕES FINANCEIRAS**

Monografia apresentada à Escola Politécnica
da Universidade de São Paulo para obtenção
do Título de Especialista em Gerenciamento
de Facilidades-MBA/USP.

São Paulo
2005

MOISES THIEME

**MODELO DE GOVERNANÇA EM FACILIDADES PREDIAIS
PARA CENTROS DE TECNOLOGIA DA INFORMAÇÃO
DE INSTITUIÇÕES FINANCEIRAS**

Monografia apresentada à Escola Politécnica
da Universidade de São Paulo para obtenção
do Título de Especialista em Gerenciamento
de Facilidades-MBA/USP.

Área de Concentração:
Gerenciamento de Facilidades

Orientador:
Prof. Dr. Marcelo Schneck de Paula Pessôa

São Paulo
2005

FICHA CATALOGRÁFICA

Thieme, Moises

Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação em Instituições Financeiras

Moises Thieme. -- São Paulo, 2005.

212 p.

Monografia (MBA em Gerenciamento de Facilidades) – Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1.Governança em TI 2.Facilidades Prediais 3. Instalações de Missão Crítica 4.CPD/Edificações I.Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II.t.

DEDICATÓRIA

Para Fabiula com todo o meu amor, o qual permanece
ainda maior do que aquele da abelha pela flor.

AGRADECIMENTOS

Ao Prof. Dr. Marcelo Schneck de Paula Pessôa, pelo acompanhamento, orientação, empenho e direção na abordagem de tema tão abrangente e complexo, cuja colaboração foi fundamental aos resultados obtidos.

Ao Prof. Dr. Moacyr Eduardo Alves da Graça, pelo incentivo, dedicação, inspiração, jornada de companheirismo e luta no estabelecimento de conceitos do Gerenciamento de Facilidades para o mercado nacional.

Aos meus pais Augusto (“in memoriam”) e Maria, pelo amor e confiança que sempre me dedicaram, pelo estímulo aos estudos, por toda a minha formação e o ensino de amor a Deus sobre todas as coisas.

A minha esposa Dra. Fabiula Ferreira Martins Thieme, pelo imenso amor, apoio em todas as horas e o suporte jurídico significativo para a conclusão deste trabalho.

A todas as pessoas queridas, pela compreensão e apoio, durante os meus estudos.

A Deus sobretudo, pela imensa graça, abundante misericórdia e grandes propósitos em me permitir trilhar este caminho de aprendizado contínuo. A Ele toda Glória e Honra por mais esta conquista em minha vida.

RESUMO

O presente trabalho estuda de maneira analítica as diversas legislações específicas de impacto no setor bancário, em face da elevada dependência de Tecnologia da Informação com a crescente demanda por aceleração do processamento de dados e elevação dos níveis internacionais de exigências nos controles de Governança Corporativa, sob uma abordagem aos conceitos necessários para o suporte e planejamento dos sistemas de Gerenciamento de Facilidades em edificações de alto desempenho e de elevada criticidade. Assim compreende, os elementos que possibilitam este entendimento e os meios necessários para atingir os objetivos propostos, incluindo análises em níveis estratégico e tático, além de contemplar questões como segurança da informação, gestão de riscos operacionais, legislações, normativas e regulamentos para auditorias de instalações, gerenciabilidade dos edifícios e seus sistemas, planejamento estratégico, diagnóstico de soluções e a efetividade de custos operacionais conjuntamente com o oferecimento de elevada disponibilidade, confiabilidade e manutenibilidade em instalações físicas de Missão Crítica. Ao final, desenvolve uma proposta de modelo para a Governança de Facilidades Prediais em Centros de Tecnologia da Informação, visando possibilitar a transição dos modelos de gestão predial, até então utilizados para a operação e manutenção nos Centros de Processamento de Dados, de maneira que, sejam reforçados os recursos para se enfrentar os novos desafios impostos às Instituições Financeiras de Classe Mundial.

ABSTRACT

The following work analyzes the key concepts, from a analytical point of view, involved in multiples specific laws and impacts in the bank sector, considering its high dependence of the Information Technology with growing demand by data processing acceleration and international high levels in compliance to Corporate Governance, through an approach that considers the concepts needed to support and planning the systems of Facilities Management for high performance and critical buildings. Both the elements that make this understanding possible and the means needed to achieve the proposed goals are analyzed according to strategic and tactical levels, including questions such as information security, operational risk management, laws, rules, facilities auditing, facilities management, strategic planning, solutions diagnoses and operational costs effectiveness to offer high availability, reliability and maintainability of the building and its systems to Mission Critical Facilities. At the end, this work proposes a model to Facilities Governance for transitional adjustments in managerial models employed so far for operating and maintaining Data Centers, so that may be reinforced resources to face the new challenges posed to the World Class Finance Organizations.

SUMÁRIO

LISTAS DE FIGURAS

LISTA DE TABELAS

RESUMO

ABSTRACT

Capítulo 1 – INTRODUÇÃO.....	1
1.1 Descrição Preliminar.....	2
1.2 Contexto Legislativo do Setor Bancário.....	5
 Capítulo 2 – PANORAMA DE TECNOLOGIA DA INFORMAÇÃO.....	 21
2.1 O Paradigma das Instituições Financeiras de Classe Mundial.....	23
2.2 Gestão de Segurança da Informação.....	26
2.3 Conceitos em Facilidades Prediais de Missão Crítica.....	40
2.4 Classificação de CPD's (Desempenho Físico).....	46
 Capítulo 3 – PLANEJAMENTO ESTRATÉGICO.....	 55
3.1 Resumo de Proposta.....	57
3.2 Metodologia-Etapas.....	62
3.3 Resultados Esperados.....	64
 Capítulo 4 – ESPECIFICAÇÕES DE PADRÕES PREDIAIS.....	 67
4.1 Diretrizes Construtivas.....	70
4.2 Fornecimento e Distribuição de Energia.....	72
4.3 Climatização, Ventilação e Resfriamento.....	94
4.4 Segurança Física.....	103
4.5 Cabeamento Lógico.....	121
4.6 Monitoração e Inteligência Predial.....	122

Capítulo 5 – REQUISITOS CONTRATUAIS AOS FORNECEDORES.....130

5.1	Projetos Conceituais e Executivos.....	134
5.2	Gerenciamento da Construção e Montagens.....	138
5.3	Cronograma, Qualidade, Testes e Garantias.....	144
5.4	Comissionamento e Testes de Aceitação.....	146
5.5	Certificação Ambiental (LEED).....	154
5.6	Operação e Manutenção do CPD.....	162

Capítulo 6 – GOVERNANÇA EM FACILIDADES PREDIAIS..... 168

6.1	Proposta de um Modelo Básico de Governança em <i>Facilities</i>	175
6.2	Ferramentas de Apoio Automatizado (CAFG/CAFM).....	178
6.3	Plano de Reestruturação da Infra-estrutura.....	182
6.3.1	Objetivos.....	182
6.3.2	Sumário Executivo.....	183
6.3.3	Nova Denominação da Área.....	184
6.3.4	Descrição de Missão e Visão.....	185
6.3.5	Redesenho de Organograma.....	186
6.3.6	Conjunto de Premissas Básicas do TI-GFAC.....	189
6.3.7	Essência da Governança em <i>Facilities</i>	190
6.3.8	Plano de Cargos e Funções.....	193
6.3.9	Consolidação.....	197

CONCLUSÃO..... 199

ANEXOS

REFERÊNCIAS BIBLIOGRÁFICAS

LISTA DE FIGURAS

Figura 1	Estrutura de Sustentação de Empresa no Setor Bancário.....	3
Figura 2	Demonstrativo de Custos Anuais de Manutenção nos EUA.....	4
Figura 3	Deficiências dos Controles por Planilhas Setoriais.....	5
Figura 4	Visões do Planejamento Estratégico.....	8
Figura 5	Fatores de Riscos e Controles da SOX.....	12
Figura 6	Estrutura de Controles Internos da SOX.....	13
Figura 7	O Modelo COSO para Governança Corporativa.....	14
Figura 8	Diagrama de Blocos dos Requisitos da Legislação.....	17
Figura 9	Estrutura de Indicadores do Desempenho da Organização.....	18
Figura 10	A Estrutura de TI nas Empresas.....	25
Figura 11	Elementos de Camadas na Estrutura de TI.....	25
Figura 12	Composição Básica de TI no Data Center.....	27
Figura 13	Ameaças ao Ambiente Físico.....	28
Figura 14	Medidas de Proteção em Data Center.....	29
Figura 15	Exemplo de CPD em Sala Cofre.....	30
Figura 16	Momento de Falência em Parada do CPD.....	33
Figura 17	Principais Componentes de um Cenário.....	56
Figura 18	Visão Total do <i>Projeto</i>	58
Figura 19	Dimensões do Diagnóstico de TI.....	60
Figura 20	Conteúdo das Propostas.....	61
Figura 21	Abordagem de Migração nas Etapas do Planejamento.....	65
Figura 22	Exemplo de Sistema Elétrico <i>Single-bus</i>	75
Figura 23	Exemplo de Sistema Elétrico <i>Dual-bus</i>	76
Figura 24	Exemplo de Sistema Elétrico <i>Three-bus</i>	77
Figura 25	Exemplo de Diagrama Elétrico em Blocos.....	80
Figura 26	Diagrama Modelo de Monitoração e Inteligência Predial.....	122
Figura 27	Diagrama Típico da Engenharia de Operações.....	163
Figura 28	Descrição do Processo de Gestão de <i>Facilities</i>	170

Figura 29	Idéia Básica de Governança em <i>Facilities</i>	176
Figura 30	Exemplo de <i>Facilities Comand Center</i>	179

LISTA DE TABELAS

Tabela 1	Velocidade de Propagação das Informações.....	41
Tabela 2	Classificação dos Elementos do Edifício.....	48
Tabela 3	Classificação Predial por Recursos do CPD.....	50
Tabela 4	Compatibilização dos Recursos de “TI & Facilities”.....	53
Tabela 5	Descritivo Básico das Principais Atividades dos Projetos.....	135
Tabela 6	Pontuação Mínima dos Níveis LEED.....	155
Tabela 7	Sistema de Pontuação do Programa LEED.....	155
Tabela 8	Níveis da Certificação LEED.....	156
Tabela 9	Crescimento da Certificação LEED.....	159
Tabela 10	Comparativo de Membros do USGBC.....	160

LISTA DE ABREVIATURAS E SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
ADR	<i>American Depositary Receipts</i>
ANSI	<i>American National Standards Institute</i>
ASHRAE	<i>American Society of Heating, Refrigerating and Air-Conditioning Engineers</i>
ASTM	<i>American Society for Testing and Materials</i>
ATS	<i>Automatic Transfer Switch</i>
BIS	<i>Bank for International Settlements</i>
BMS	<i>Building Management System</i>
CAD	<i>Computer Aided Design</i>
CAFG	<i>Computer Aided Facilities Governance</i>
CAFM	<i>Computer Aided Facilities Management</i>
CAFS	<i>Computer Aided Facilities Suppliers</i>
CD	<i>Compact Disk</i>
CEO	<i>Chief Executive Officer</i>
CFO	<i>Chief Finance Officer</i>
CFTV	Circuito Fechado de Televisão
CIO	<i>Chief Information Officer</i>
CMM	<i>Capability Maturity Model</i>
CMMS	<i>Computerized Maintenance Management System</i>
COBIT	<i>Control Objectives for Information and Related Technology</i>
COSO	<i>Committee of Sponsoring Organizations</i>
CPD	Centro de Processamento de Dados
CREA	Conselho Regional de Engenharia, Arquitetura e Agronomia
CVM	Comissão de Valores Mobiliários
DASD	<i>Direct Access Storage Device</i>
DRI	<i>Disaster Recovery Institute</i>
EIA	<i>Electronic Industries Alliance</i>

EUA	Estados Unidos da América
FMC	Facilidades de Missão Crítica
GF	Gerenciamento de Facilidades
GPS	<i>Global Position System</i>
HVAC	Heating Ventilation Air Conditioning
IAQ	<i>Indoor Air Quality</i>
ISO	<i>International Standard Organization</i>
ITIL	<i>Information Technology Infrastructure Library</i>
IEC	<i>International Electrotechnical Commission</i>
IFMA	<i>International Facility Management Association</i>
KA	Kiloampère
KVA	Kilovoltampère
KW	Kilowatt
LAN	<i>Local Area Network</i>
MAPS	<i>Methods and Procedures System</i>
MCF	<i>Mission Critical Facilities</i>
MVA	Megavoltampère
NFPA	<i>National Fire Protection Association</i>
PDU	<i>Power Distribution Unit</i>
PVC	<i>Poly Vinyl Chloride</i>
QTA	Quadro de Transferência Automática
RAID	<i>Redundant Array of Independent Disks</i>
RPP	<i>Remote Power Panel</i>
SEC	<i>Securities and Exchange Commission</i>
SOX	<i>Sarbanes Oxley Act</i>
SPDA	Sistema de Proteção contra Descargas Atmosféricas
STS	<i>Static Transfer Switch</i>
TI	Tecnologia da Informação
TIA	<i>Telecommunications Industry Association</i>
TI-GFAC	Gerenciamento de Facilidades em Tecnologia da Informação
TN	Tecnologia do Negócio
TVSS	<i>Transient Voltage Surge Supression</i>

UPS	<i>Uninterruptible Power System</i>
UTP	<i>Unshielded Twisted Pair</i>
WAN	Wide Area Network
XLPE	<i>Maximum Load Poly Ethylene</i>

Capítulo 1 – INTRODUÇÃO

O ano de 2005 marca o centenário de dois dos monumentos mais impressionantes já erigidos pelo esforço humano, monumentos que não são prédios, pontes, sinfonias ou estátuas, mas sim idéias, que, como a música de Mozart e as esculturas de Michelângelo, fizeram de seu autor um nome conhecido em todo o mundo – Albert Einstein. Em 1905, o então jovem cientista entrou para a história quando apresentou seus monumentos ao mundo – a Teoria da Relatividade Especial e a Teoria Quântica da Luz – estabelecendo uma nova era para a ciência, a qual, havia experimentado um momento anterior equivalente em importância no ano de 1666, quando Isaac Newton desenvolveu o Cálculo Diferencial e Integral, estudou a natureza da luz e lançou as bases do que viria a ser a Lei da Gravitação Universal. Assim, seria justo dizer que, entre o século XVII e o início do século XX, a humanidade viveu numa Era de Newton e, desde 1905, tem vivido a Era de Einstein, portanto, o legado deste famoso cientista foi considerado em muitas invenções – o GPS; a tela de computador; a televisão; as usinas nucleares; o CD player; a tomografia computadorizada; as armas atômicas. A ciência evoluiu distribuindo avanços tecnológicos por toda parte, o qual também encontra-se incorporado aos edifícios e seus sistemas, sobretudo na última década onde aumentaram significativamente a complexidade e a interdependência dos diversos elementos presentes no espaço construído.

Ao mesmo tempo, o mundo em que vivemos tornou-se extremamente mutante, verificando-se rápidas mudanças de valores, paradigmas e cenários, como a internacionalização dos mercados que trouxe consigo o aumento da competitividade, implicando em maior efetividade na gestão de todos os custos participantes dos processos produtivos. A chegada da nova economia, denominada de a sociedade do conhecimento*, estabelece que a informação constitui-se o único recurso

* sociedade do conhecimento = termo para definir as transformações do mundo globalizado pela tecnologia da informação, utilizado por diversos autores renomados tais como : Peter F.Drucker, Peter Senge, Schumpeter, Witzel e outros.

significativo, ao lado dos tradicionais fatores de produção – trabalho, terra e capital, cujas transformações que esse processo traz são rapidamente absorvidas pelos usuários de TI e implicam em constante elevação da demanda por inovação, segurança e garantias de continuidade do processamento e comunicação de dados.¹

Em um cenário de globalização das economias, as informações assumiram um papel estratégico nas negociações e nos processos de concorrência por mercado, levando a empresa moderna a prestar atenção especial à sua criticidade, disponibilidade, integridade e, por consequência, à segurança física dos meios magnéticos utilizados, afim de responder às mais diversas exigências de legislações específicas, órgãos reguladores e auditorias independentes que visam identificar todas as medidas tomadas para garantir os dados necessários para a concretização dos negócios.

Neste capítulo, as abordagens visam descrever os elementos introdutórios que permitem analisar o contexto legislativo do setor bancário e lançar as bases iniciais que são fundamentais ao desenvolvimento da proposta de um modelo de Governança em Facilidades Prediais de Missão Crítica, considerando os diversos paradigmas da Governança Corporativa e de Tecnologia da Informação, a globalização e o grande desafio de atender as demandas dos usuários *em harmonia de inter-relacionamento indissociável entre o homem, o edifício e o meio ambiente*², ao mesmo tempo, em que são alvos dos novos processos regulatórios deste mercado.

1.1 Descrição Preliminar

Durante a última década o ambiente de trabalho sofreu profundas transformações, bem como a maneira pelas quais as atividades são executadas, trazendo para o cenário dos tempos modernos as diversas novas maneiras de comunicação e um

volume cada vez maior de pessoas interagindo, utilizando-se de telefones celulares, teleconferência, fac-símile, correio eletrônico, computadores portáteis, internet, intranet, extranet, e tantos outros meios que aumentam consideravelmente a importância do tempo, obrigando ao aprendizado de novas formas de viver e trabalhar. Neste contexto, um dos mais importantes produtos a ser oferecido aos usuários de um edifício de alto desempenho passa a ser o acesso à informação, que possui tanto componentes intangíveis, como a própria informação, quanto tangíveis como os meios físicos por onde ela é transmitida, armazenada e manipulada, assim, também no gerenciamento de facilidades a informação, que a princípio precisa ser gerenciada, é ao mesmo tempo a maior ferramenta necessária a sua própria gestão.³

Desta maneira, o Gerenciamento de Facilidades Prediais (“Facilities Management”) pode ser entendido como a **“Interação PPP - Pessoas, Processos e Propriedades”**, os pilares principais de sustentação da Instituição Financeira de Classe Mundial, apoiados em bases fundamentais tais como os investimentos contínuos em Tecnologia, melhoria do Clima Organizacional, controle de Capital e alinhamento às Políticas/Mercados, conforme ilustração abaixo que consta da Figura 1.

Figura 1 – Estrutura de Sustentação de Empresa no Setor Bancário

Fonte : AUTOR



Os ativos físicos tais como propriedades, edifícios, equipamentos, materiais e móveis, representam uma porcentagem importante do valor total dos ativos de uma organização, os quais são utilizados por muitas unidades de negócios, departamentos e indivíduos, assim, devem ser gerenciados buscando estender seu ciclo de vida útil e minimizar seus custos de operação, como podemos perceber em pesquisas realizadas nos EUA pelo IFMA-*International Facilities Management Association*, conforme demonstrado na Figura 2, na qual fica evidenciada a importância de um efetivo controle de custos devido ao relevante percentual de participação nos ativos totais e significativos montantes envolvidos.⁴

Figura 2 – Demonstrativo de Custos Anuais de Manutenção nos EUA

Fonte: IFMA



Um modelo de estrutura para o Gerenciamento de Facilidades Prediais, contando com elevado nível de automatização de seus processos e controles, pode ser capaz de tornar disponível um sistema de informações executivas de fácil acesso e que permita eliminar as “ilhas de informações” produzidas por um “exército de planilheiros”, consolidando resultados e coordenando as atividades de diversos departamentos envolvidos na gestão corporativa, produzindo um campo fértil para o desenvolvimento de Planejamento Estratégico e de Indicadores de Desempenho no

uso dos espaços físicos, visando tratar as deficiências de fluxo das informações e controles setoriais, conforme demonstrado na Figura 3 a seguir.⁵

Figura 3 – Deficiências dos Controles por Planilhas Setoriais

Fonte : AUTOR



Exército de Planilheiros

- **Fragilidade**
- **Não Colaborativo**
- **Manutenção Intensiva**
- **Controle Pouco Centralizado**
- **Consolidação Não Gerenciável**
- **Pobreza na Integração de Dados**



Disponer facilmente de um histórico de informações torna mais simples a previsão dos custos futuros e a criação de planos orçamentários, contendo previsões financeiras através de avaliações das condições, análise de valor e desempenho dos ativos físicos, bem como favorece o cumprimento de normativas das agências regulatórias e a gestão do volume de trabalho.

1.2 Contexto Legislativo do Setor Bancário

Uma das atividades mais importantes das empresas direta ou indiretamente envolvidas com o mercado financeiro é a gestão do risco de crédito, risco de

mercado, risco operacional e gestão profissional de outros riscos. A exposição a esses riscos não pode permitir a desestabilização dos mercados. O novo Acordo de Capital da Basileia, também conhecido como Basileia II é uma das atuais prioridades do mercado financeiro e, muito embora os novos requisitos ainda não estejam finalizados, as principais implicações para os bancos e instituições financeiras já estão bastante claras. As novas normas impostas pelo Acordo de Capital da Basileia II não só passarão a assegurar o alinhamento dos níveis de capital dos bancos com sua exposição ao risco, como passarão a exigir que os bancos controlem os riscos de forma adequada, justificando cada risco no qual irão incorrer e serão futuramente alvo de divulgação ao mercado. Isto significa que os bancos deverão estar em conformidade com os rigorosos padrões ditados pelos reguladores, depositários e pelo próprio mercado. Essas medidas afetam diretamente a qualidade das informações e a integração dos sistemas, interferindo consequentemente, em todo o ambiente de TI, cujo principal desafio encontra-se em oferecer uma infra-estrutura capaz de suportar os processos na área de gestão do risco operacional. O prazo para que as normas do Acordo Basileia II sejam incorporadas à legislação nacional ainda parece distante, entretanto, pela complexidade deste cenário todos os bancos e instituições financeiras devem assegurar que seus sistemas estejam totalmente implementados e compatíveis no momento em que as novas regulamentações sejam levadas a efeito.⁶

O que são dados? Eles são ativos da empresa? Podemos conferir a eles o valor de patrimônio ou são meras informações? Muitas vezes os dados são provas de relações geradas eletronicamente, quer seja o conteúdo da obrigação gerada ao se transmitir um e-mail até mesmo a conversa entre computadores que estão autenticando a entrada de um usuário no sistema, e, portanto, confere a ele poderes para ir e vir na rede digital, da intranet até a internet, passando por redes wireless, extranets e tudo o mais de tecnologias que seja possível inventar. A sociedade atual é uma sociedade de dados, tanto a identidade como o dinheiro são dados eletrônicos que estão cada vez mais ameaçados por conta de fraudes digitais e como bens intangíveis são alvos de cobiça por parte daqueles que até então tinham de furtá-los ou roubá-los de nós de modo presencial e perigoso no mundo real, sendo que a tecnologia veio para

colaborar para que isto agora possa ocorrer de modo indolor e até divertido através de interfaces gráficas amigáveis e e-mails inofensíveis que exploram a vontade de se ter fama ou de ganhar algo fácil. Os riscos operacionais de que trata o Acordo de Basiléia II vem justamente de encontro com a preocupação cada vez maior com a situação de controle e proteção dos dados nas empresas, sendo esta responsabilidade a prioridade da pauta de governança corporativa e pública, uma vez que estes são depositários fiéis dos dados de terceiros, quer sejam funcionários, colaboradores, fornecedores ou parceiros. O modelo de negócios atual exige uma cadeia complexa de conectividade interoperacional entre todos os participantes e a falta de diligência ou a negligência no trato das informações por parte de um pode contaminar a todos.

O Acordo de Basiléia II tem impacto relevante no cenário brasileiro porque a origem da maioria das recentes perdas incorridas pelas Instituições Financeiras é operacional por natureza e a magnitude desses incidentes podem causar sérios problemas ao negócio ou até mesmo o seu colapso, portanto, esta perspectiva gera uma preocupação de se revisar os conceitos para o controle de riscos operacionais em bancos, operadoras de cartão, financeiras, corretoras e seguradoras. Saber mensurar e minimizar o risco operacional torna-se uma variante essencial e gera a necessidade de implementar Estratégias, Métodos, Estruturas e Sistemas onde se é preciso ter histórico do que deve ser guardado e por quanto tempo, cujos prazos legais podem ser de no mínimo 1 ano (consumidor) até 10 anos (penal), podendo chegar até 50 anos em alguns casos. Devido a uma questão de prova jurídica, o Acordo Basiléia II traz também a necessidade de criação e manutenção de uma Base Histórica de Dados, portanto, para mitigar risco é necessário identificá-lo, avaliar o seu impacto financeiro, bem como a sua probabilidade de ocorrência nos diversos processos da empresa, logo, é necessário a estruturação de uma base histórica de dados que sustente uma projeção segura das possíveis perdas futuras, ou seja, o passado deve ser alvo de registro consistente para melhor se projetar o futuro como demonstra o ilustrativo da Figura 4.⁷

Figura 4 – Visões do Planejamento Estratégico*Fonte : AUTOR*

Vivemos uma realidade nova onde um simples e-mail pode representar uma grande obrigação e responsabilidade legal, com possíveis contingências até mesmo financeiras, custos e riscos que podem atingir não apenas o bolso, mas principalmente a reputação das empresas e suas marcas e, neste sentido, o Novo Código Civil também ampliou as responsabilidades dos administradores. Além disso, torna-se preciso investir em educação, pois apesar da tecnologia, os erros humanos devem ser previstos em processos, anúncios e mensagens que chamam a atenção para não se cair em pegadinhas de engenharia social, portanto, há uma enorme responsabilidade das empresas em se criar uma cultura de segurança que vai além de se pensar apenas em senhas de acessos.

O Acordo de Basileia II enfoca os dois modos conhecidos do setor bancário ganhar dinheiro – oferecendo serviços a clientes e arriscando (como se diria antigamente “no arriscar é que está o ganho”) – assim, os bancos aceitam os depósitos dos clientes e, em troca, oferecem-lhes garantias de clareza e segurança na armazenagem do dinheiro, ou seja, os riscos para o setor bancário ocorrem quando estes assumem empréstimos individuais, correndo o risco de que não sejam reembolsados total ou parcialmente e, na sua maioria, os bancos estão dispostos a correr riscos, cobrando

em retorno uma elevada taxa de interesse. Geralmente, quanto maior o risco que os bancos assumem mais dinheiro esperam ganhar, no entanto, quanto maior é esse risco, maior é a probabilidade de os bancos perderem em larga escala e serem obrigados a sair do setor bancário. Assim sendo, os bancos tentam assegurar que o risco assumido por eles é informado e prudente, desta forma, o controle deste “jogo” constitui-se o negócio da Gestão de Risco, cuja atuação pode ser enquadrada em três categorias distintas : ⁸

- a) **Risco de Mercado** – advém da possibilidade de ocorrerem perdas mediante movimentos desfavoráveis no mercado. É o risco de perder dinheiro resultante da mudança ocorrida no valor percebido de um instrumento, cujo exemplo clássico são as perdas na Bolsa de Valores;
- b) **Risco de Crédito** – ocorre quando pessoas individuais, empresas ou o governo falham em honrar o compromisso assumido de efetuar um pagamento. Este tipo de risco advém de diversas fontes, entre as quais podemos destacar os empréstimos individuais (falha em repor total ou parcialmente a quantia emprestada) e as operações de troca (quando o sujeito percebe que vai perder dinheiro com a troca e fica relutante em pagar);
- c) **Risco Operacional** – compreende todas as outras formas, a partir das quais é possível que um banco perca dinheiro. É o risco de perdas diretas ou indiretas resultante de inadequação ou falha dos processos internos, pessoas e sistemas ou em face de eventos externos, cujo exemplo típico é a fraude.

Em contrapartida às novas pressões de mercado e aos escândalos financeiros ocorridos em anos passados, tornou-se eminente impulsionar todos os bancos em nível mundial a possuírem um sistema de informação que lhes permitisse gerir o risco de maneira eficaz, assim, a entidade responsável BIS-*Bank for International Settlements* lançou uma proposta para um acordo de capital que se assenta em três pilares dependentes que permitem aos bancos e seus supervisores avaliarem corretamente os tipos de riscos nas três categorias descritas acima, o qual foi denominado de Acordo Basiléia II, cujo pilar do Risco Operacional encontra no Gerenciamento de Facilidades Prediais um grande aliado para o controle eficiente e

eficaz dos requisitos inclusos nesta normativa de âmbito internacional. No final do ano de 2006, os bancos deverão estar funcionando de acordo com a regulamentação do Acordo de Basiléia II e, muito embora esta data possa estar sujeita a alterações, atualmente já é uma preocupação de negócio encarada por bancos em todo o globo, em todos os seus níveis hierárquicos, cuja implementação correta e inteligentemente efetuada poderá também contribuir para reduzir as reservas necessárias de capital, aumentando a quantia de recursos disponíveis para investimentos nos bancos e, conseqüentemente, contribuindo para aumentar o valor do patrimônio de acionistas e os níveis de lucro através de uma gestão de riscos aperfeiçoada de relevante interdependência junto a Gestão de Facilidades Prediais.

Não obstante as exigências do Acordo Basiléia II, os escândalos financeiros de grandes empresas nos Estados Unidos (EUA) também alteraram radicalmente as regras no mundo dos negócios para as empresas que possuem os ADR-*American Depositary Receipts*, levando ao aperfeiçoamento dos padrões contábeis, provocando mudanças na responsabilidade dos administradores das companhias e na forma com que as empresas tratam os acionistas minoritários e prestam contas ao mercado, tudo isso como novidades que constam da lei norte-americana “Sarbanes Oxley Act” imposta a todas as corporações americanas e inclusive estrangeiras, com ações negociadas nas bolsas de valores dos EUA.

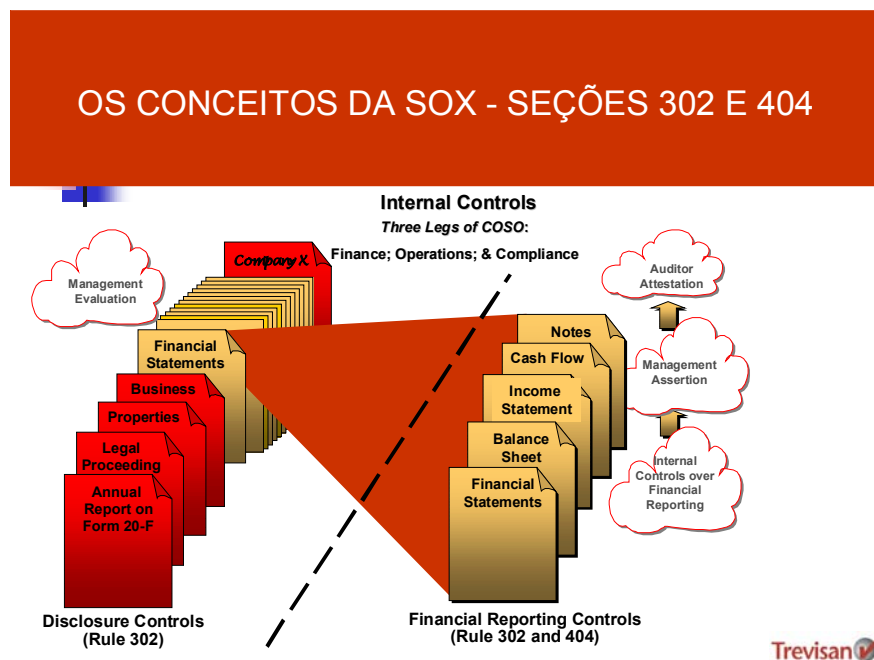
Aprovada em janeiro de 2002, logo após a descoberta do primeiro grande caso de fraude, o da gigante elétrica Enron e depois seguido pelos casos da WorldCom e Arthur Andersen, a lei Sarbanes-Oxley, uma referência aos dois membros do congresso norte-americano responsáveis pela sua elaboração – o senador democrata Paul Sarbanes e o deputado republicano Michael Oxley – configurou-se na mais importante reforma da legislação de mercado de capitais dos EUA desde a introdução de sua regulamentação na década de 30, após a quebra da Bolsa de Nova York em 1929. Não há dúvidas sobre a dimensão da lei “Sarbanes-Oxley ou “Sarbox” ou ainda simplesmente “SOX” (como foi apelidada pelos americanos) ou “SOA” (sigla para o “Sarbanes Oxley Act”) e sobre as mudanças radicais que ela provocará na teia de relações tecida pelas empresas, pois a lei foi uma resposta dos

políticos aos milhões de investidores e eleitores americanos que viram suas ações “micarem” por causa de fraudes contábeis em corporações americanas consideradas sólidas.⁹

Uma das premissas da SOX é que as empresas demonstrem eficiência na Governança Corporativa, sendo uma referência nessa área o modelo norte-americano que leva o nome da entidade que o criou COSO-*Committee of Sponsoring Organizations of the Treadway Commission* criado em 1985 para definir processos de controle interno das empresas. O COSO define que o controle interno é um processo e deve ser exercido por todos os níveis da empresa, o qual deve ser desenhado para atingir os seguintes objetivos : (i) efetividade e eficiência na operação; (ii) dar confiabilidade nos relatórios financeiros; e, (iii) atender as leis e regulamentações dos órgãos públicos. As principais novidades da Sarbanes-Oxley (SOX) estão ligadas às exigências de criação de um comitê de auditoria, desenvolvimento de controles internos pelas empresas para a verificação das informações a serem divulgadas e responsabilidade dos executivos e dos auditores externos em relação aos números apresentados pelas companhias. O aprimoramento dos controles internos é um grande desafio para as empresas, cujo trabalho envolve identificar as áreas de negócio, documentar processos e garantir que as informações precisas e corretas fluam até chegar à administração da companhia, responsável pelos resultados financeiros, assim, a SOX requer que, além de desenvolver os controles, os executivos (presidente e diretor financeiro) analisem e certifiquem o desenho e a operação dos mecanismos, havendo ainda a exigência de que o auditor externo certifique a avaliação da administração e emita um relatório. Podemos perceber a importância da Governança Corporativa e a abrangência do modelo COSO no controle interno de processos das empresas, conforme demonstrado a seguir na Figura 5.¹⁰

Figura 6 – Estrutura de Controles Internos da SOX

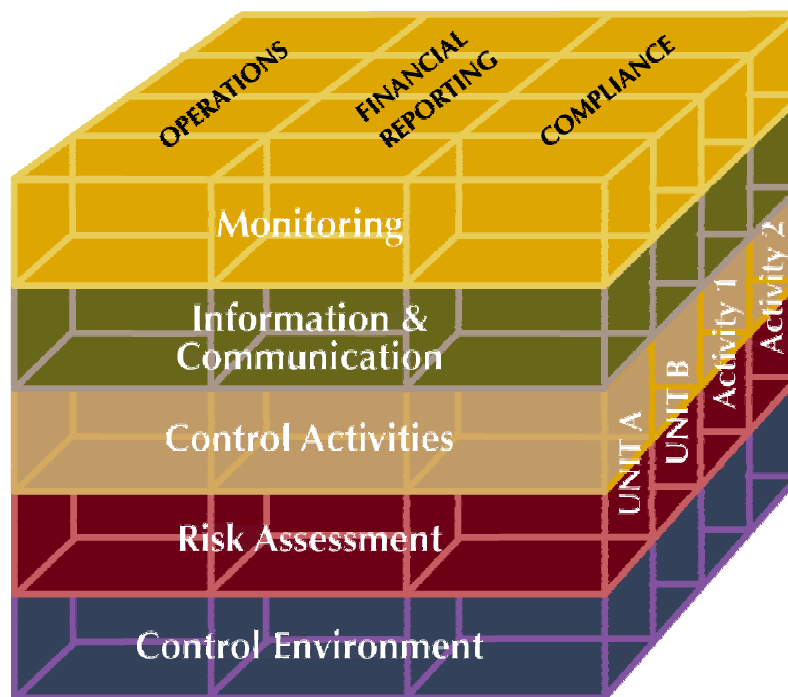
Fonte : TREVISAN



Os bancos brasileiros estão mais preparados do que as empresas nacionais para a adaptação à lei norte-americana Sarbanes-Oxley (SOX), isso porque já cumprem uma série de normas do Banco Central que se assemelham às dos Estados Unidos e do próprio órgão regulador do mercado nacional, a CVM-Comissão de Valores Mobiliários que tem aproveitado as idéias da SOX para fazer ajustes nas suas normas, mas ainda falta muito para as empresas brasileiras com ações negociadas nos Estados Unidos cumprirem as exigências desta nova lei, principalmente no modo como administram seus ativos físicos no modelo atual de Gestão de Infra-estrutura e Instalações que são fundamentais à primeira camada base de sustentação das empresas – a Tecnologia da Informação – cujo conteúdo deve atender ao modelo COSO de Governança Corporativa, conforme descrito a seguir na Figura 7.

Figura 7 – O Modelo COSO para Governança Corporativa

Fonte : COSO



Nesse contexto, a área de Tecnologia da Informação (TI) tem um papel importante, onde o próprio COSO faz um comentário especial recomendando que TI deve cobrir todos os aspectos de segurança e controle das informações digitais da empresa, devendo desenhar processos de controle das aplicações para assegurar a confiabilidade do sistema operacional, a veracidade dos dados de saída e a proteção de equipamentos e arquivos.

Para cumprir essas exigências os CIO-*Chief Information Officer* (o mais alto posto da hierarquia no segmento de TI da empresa) devem rever todos os processos internos cobrindo desde as metodologias de desenvolvimento de sistemas até as áreas de operações de computadores, promovendo uma conscientização nas áreas usuárias de seus recursos sobre aspectos de segurança e cuidados na manipulação das informações, tais como : e-mails, compartilhamento de diretórios nos PC-Personal Computers (computadores pessoais), compartilhamento de senhas de acesso aos aplicativos e estes aspectos de engenharia social também devem ser reforçados para

o pessoal de TI, que as vezes não conseguem determinar os riscos de segurança em suas soluções. Visando atender aos novos desafios da Governança Corporativa, as áreas de TI contam com alguns modelos de gestão que se aplicados asseguram a conformidade com as melhores práticas de processos e segurança da informação, os quais podem ser listados conforme segue : ¹¹

- (1) COBIT - *Control Objectives for Information and Related Technology* para a Governança em TI;
- (2) ITIL - *Information Technology Infrastructure Library* para a Gestão de Serviços em TI;
- (3) DRI - *Disaster Recovery Institute International* para a Especificação e Operação de Planos de Continuidade de Negócios;
- (4) ISO-*International Standard Organization* NBR ISO/IEC 17799:2005 e ISO 27001:2005 para a Gestão de Segurança da Informação;
- (5) CMM - *Capability Maturity Model* que define um modelo de Gestão para o Desenvolvimento de Software.

Dentre os requisitos destas normativas, há um enfoque crucial para o Gerenciamento de Facilidades Prediais cujos requisitos apontam para a necessidade de um modelo que proporcione uma Gestão Completa de Infra-estrutura e Instalações como fator de otimização do desempenho de negócios das empresas, tanto pela relevância financeira dos ativos físicos - propriedades, edificações, equipamentos e instalações – na redução dos ativos fixos totais da empresa, como pela capacidade de gerar segurança das informações através de relatórios gerenciais precisos e rápidos, contendo gráficos dos processos de negócios e dos ativos físicos, utilizados para atender os requisitos de auditorias internas e externas em face de rígidas legislações como a SOX.

No Brasil também podemos identificar vários fatores de influência ao contexto legislativo para o setor bancário, cujos requisitos implicam em melhorias do Gerenciamento de Facilidades Prediais, pois a evolução tecnológica contribuiu para o desenvolvimento de uma sociedade mais informada e também mais exigente, não só relativamente ao funcionamento dos edifícios e seus sistemas, mas também no que

diz respeito ao cumprimento de leis, normas, códigos e regulamentos. Assim, podemos relacionar uma série de novos dispositivos que elevaram o nível de exigências e de impactos significativos nos controles de riscos operacionais, tais como :

- Efeitos e conseqüências das legislações internacionais, como a Sarbanes-Oxley e Basiléia II, as quais implicaram no desenvolvimento de diversos dispositivos nacionais para a melhoria dos controles e a criação de um Código das Melhores Práticas em Governança Corporativa, tais como : Cartilha CVM, CM 3041, CVM 404/308/358, CVM Ofício Circular 01/04, Bovespa Novo Mercado e a Lei das Falências;
- Os requisitos das normas sobre Gestão de Segurança da Informação, ISO 27001:2005 e NBR ISO/IEC 17799:2005;
- Edição da Lei 8.078 em 11 de setembro de 1990, conhecida como “Código de Defesa do Consumidor (CDC)”, ponto marcante na mudança dos padrões de exigências dos consumidores, em cujo artigo 39, inciso VIII, atribui a força de lei às normas técnicas expedidas pelos órgãos oficiais competentes ou pela ABNT- Associação Brasileira de Normas Técnicas ou outra entidade credenciada pelo CONMETRO-Conselho Nacional de Metrologia, Normalização e Qualidade Industrial;
- Edições da Portaria 3.523 de 28 de agosto de 1998 e da Resolução 09 de 16 de janeiro de 2003 do Ministério da Saúde (MS) através da ANVISA-Agência Nacional de Vigilância Sanitária, cujos textos atribuíram exigências severas para o controle de qualidade e climatização de ar de interiores em edifícios comerciais;
- Os requisitos de qualidade das normas NBR-ISO 9001(2000), ISO 9002(1997), ISO 14001(2004) e ISO 18001 (2002), as quais passam a ser determinantes para o acesso a muitos mercados, em face da globalização;
- Os regulamentos do MTE – Ministério do Trabalho e Emprego sobre os SSMT-Serviços de Segurança e Medicina do Trabalho, tais como a NR10:2004 sobre as Instalações e Serviços em Eletricidade que atribuem um rigoroso plano de controle destes, principalmente nos requisitos para os controles de riscos e

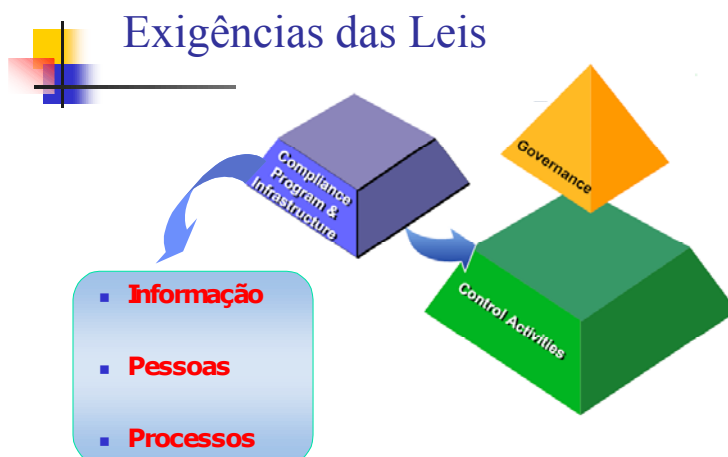
“Proteção contra Choque” especificados na NBR 5410:2004-Instalações Elétricas de Baixa Tensão;

- Edição do Decreto-Lei Estadual 46.076 de 31 de agosto de 2001 que trata da Segurança contra Incêndios em edificações comerciais;
- Edição da Lei 10.406 de 10 de janeiro de 2002 conhecida como “Novo Código Civil” que atribui maiores exigências e controles para as empresas S/A;
- Edição da Decreto-Lei Estadual 5.269 de 02 de dezembro de 2004 que trata as questões de Acessibilidade em edifícios comerciais;
- Decreto Lei 2.848 de 1940 conhecido como “Código Penal”, cujo artigo 132 atribui crime e penas aplicáveis ao fato de se “expor a vida ou saúde de outrem a perigo direto e iminente”, cujo texto ganha uma nova força frente as legislações sobre instalações elétricas, segurança contra fogo, ar-condicionado e acessibilidade citadas acima, bem como todas as demais normativas técnicas elevadas à condição de regulamentos com poder de lei, em face do Código de Defesa do Consumidor (CDC);

O conjunto de requisitos presente nos diversos dispositivos da legislação internacional e suas complementares em âmbito nacional conforme as referências citadas, visam proporcionar a elevação do nível de controles internos da organização, conforme descrito no diagrama que consta da Figura 8 abaixo.

Figura 8 – Diagrama de Blocos dos Requisitos da Legislação

Fonte : IT GOVERNANCE INSTITUTE



A adequação a todos estes padrões internacionais e nacionais com impactos no setor bancário, seus recursos de TI e de ambientes físicos de trabalho, trazem um custo extra às empresas, entretanto, no médio e longo prazos esses controles passam a ser um diferencial positivo para atrair novos investimentos e proporcionar maior segurança aos acionistas, ao estabelecer padrões e processos que permitam criar a estrutura de desempenho descrita a seguir na Figura 9.

Figura 9 – Estrutura de Indicadores do Desempenho da Organização

Fonte : IT GOVERNANCE INSTITUTE



Não obstante o contexto legislativo aplicável de forma compulsória ao setor bancário, refletindo um conjunto de exigências que constam de normativas internacionais que imprimem os seus reflexos e geram complementos normativos em âmbito nacional, ainda se faz presente um novo conjunto de requisitos de ordem na responsabilidade social e ambiental, em face de aderência voluntária aos mecanismos da política de sustentabilidade, a qual oferece valor agregado real e torna urgente a sua incorporação estratégica nas organizações, tais como o "EQUATOR PRINCIPLES" (Princípios do Equador) e o "GLOBAL COMPACT" (Pacto Global) adotado por várias Instituições Financeiras de Classe Mundial.

As políticas de sustentabilidade concorrem para a dinâmica de valorização dos ativos intangíveis empresariais, erguendo-se como elementos de aumento da competitividade e fator de melhoria do desempenho, evocando cenários e objetivos de perpetuação e crescimento das organizações e de sua rentabilidade financeira. Assim, trata-se de estimular a integração consciente de estratégia empresarial, desempenho ambiental e responsabilidade social, numa realidade unificada e harmônica, em busca de sucesso na tríplice linha do resultado final que engloba as dimensões econômicas, ambientais e sociais como veículos de agregação de valor, cujos fatores impulsionam a criação de um quadro de impactos relevantes na elevação de influências externas para os demonstrativos de controles internos e gestão de riscos operacionais, os quais, em última análise, dependem da “Gestão Completa de Infra-estrutura e Instalações”.

O mundo tem assistido, especialmente nos Estados Unidos e Europa, ao crescimento vertiginoso dos fundos de SRI-*Socially Investment Funds* que passam a ser expressão de uma dinâmica de evolução, em que a inicial pressão das organizações não governamentais é agora substituída pelas escolhas conscientes de investidores institucionais e fundos de pensão, em busca de uma melhor e mais segura rentabilidade financeira, representando avaliações de cunho ético, ambiental e social que nos EUA já atingem pelo menos um em cada oito dólares investidos, acarretando uma definitiva e paralela consolidação de outros fenômenos incipientes, como a multiplicação de novas empresas e entidades de avaliação do desempenho sócio-ambiental, cujos reflexos encontram-se ora ampliados pelo setor bancário.⁷

No tocante às instituições financeiras, o *Equator Principles*, assinado em junho de 2003, tem aglomerado um número crescente de bancos internacionais de primeira linha, ao redor do empenho de incluir a variável sócio-ambiental nas atividades de *project finance* e concessão de crédito para projetos de valor superior a cinquenta milhões de dólares, em conformidade com as diretrizes formuladas pelo IFC-*International Finance Corporation* do Banco Mundial. A amplitude do fenômeno em tela permite vislumbrar um processo de mudança dos paradigmas corporativos, levando para a agenda dos tomadores de decisões as questões de responsabilidade

social e governança corporativa, da eco-eficiência e da própria redução dos gases de efeito estufa, assim, cada vez mais freqüentemente são idealizados indicadores, iniciativas de mensuração e certificação nas práticas globais de sustentabilidade que estão progredindo rapidamente para um conceito de obrigatoriedade, os quais podem suportar o consumidor na identificação de produtos e serviços mais compatíveis como o meio ambiente e socialmente justos.¹²

Assim concebidas, as políticas voluntárias de sustentabilidade e a aderência compulsória ao novo contexto legislacional aplicável ao setor bancário, bem como a visão de controles internos na gestão de riscos, mais especificamente neste trabalho o enfoque de riscos operacionais, constituem-se instrumentos focais e privilegiados de administração dos ativos empresariais, sobretudo nesta abordagem dos ativos físicos de infra-estrutura e instalações, cujo instrumentário deve ser formado por uma série de valores e atitudes que transitam pela eficiência de gestão, inovação contínua, ética em todas as relações, diálogo incessante, transversalidade das intervenções, transparência das informações (“*disclosure*”) e integração dos conhecimentos, cuja implementação na visão estratégica de longo prazo implica em adoção de abordagens inovadoras que permitam proporcionar mudanças nos padrões de pensamento, partindo-se da “ética do custo” rumo a “ética do investimento”.

Assim, neste capítulo tivemos alguns indicadores situacionais de contexto do setor bancário no tocante aos impactos de legislações, normativas e regulamentos na gestão dos serviços de tecnologia da informação, sobretudo em abordagens que constituíram os elementos fundamentais de Governança Corporativa e Governança em TI que preconizam e alicerçam as bases para uma proposta de modelo de Governança em *Facilities* que trataremos neste trabalho.

Capítulo 2 – PANORAMA DE TECNOLOGIA DA INFORMAÇÃO

Neste capítulo, o enfoque recai sobre as mais recentes demandas para a Tecnologia da Informação, cujo panorama inclui um posicionamento situacional, análises sobre a gestão de segurança da informação e conceitos em Facilidades Prediais de Missão Crítica nos ambientes de centros de processamento e comunicação de dados em Instituições Financeiras de Classe Mundial.

O setor bancário encontra-se num momento decisivo de grande transformação do mercado e, mais do que nunca, vale lembrar uma máxima tantas vezes citadas nesse meio que diz “a única coisa que nunca muda é a necessidade de mudanças”. No caso dos bancos quando se diz que precisam conhecer e entender, cada vez mais, o negócio dos seus clientes, na verdade, o enfoque recai sobre o profissional bancário que deve estar num ciclo virtuoso de capacitação contínua para realizar esta tarefa. A transformação no mercado bancário é, em essência, uma transformação dos profissionais que atuam neste segmento imerso em sofisticada estrutura tecnológica e a informatização de atividades está em constante evolução – as funções repetitivas sendo substituídas por máquinas ou terceirização – exigindo um esforço constante, mas significando oportunidades no contexto de mudanças, cujo perfil faz com que os bancos tenham de investir muito mais do que fazem hoje em desenvolvimento de novas soluções tecnológicas.

Desta maneira, os bancos encontram sua nova identidade na busca permanente por mudanças em face de grandes transformações na forma de operação devido a economia digital. Nos últimos cinco anos, as grandes empresas foram surpreendidas com a introdução de tecnologias que não haviam sido consideradas em seus planos estratégicos, como em 1996 quando muitos acreditavam que a Internet era irrelevante, do ponto de vista de negócios, e que não teria efeito significativo no comportamento dos clientes. Em 1999, o mercado se rendeu a nova realidade e chegou-se a conclusão de que a Internet era inexorável e aqueles que estavam

atrasados decidiram investir muito para tentar recuperar o terreno perdido. Em 2001, houve nova mudança de idéia, a Internet era importante mas não tanto e tudo parecia ser o resultado de uma bolha tecnológica e se deveria gastar o mínimo possível.⁶

Nesse quadro de alterações constantes no mercado, quais serão os possíveis erros dos bancos do futuro? Haverá o reconhecimento de que a economia digital transformou as finanças corporativas? Novas tecnologias serão sempre bem vindas para quem as usa e o objetivo é sempre melhorar o desempenho, facilitar a tomada de decisões e remover a necessidade de inúmeras intervenções humanas. Se a tecnologia é boa e funciona, alguém vai copiar a idéia e produzir algo melhor e mais barato, assim, é muito difícil para uma Instituição Financeira de Classe Mundial manter a vantagem competitiva com o uso de tecnologia, se não estiver constantemente inovando e investindo. Todas as disciplinas do banco corporativo serão transformadas pelas novas tecnologias e com a criação de novos produtos, os canais de distribuição e a natureza do relacionamento com os clientes serão afetados, portanto, as melhores instituições serão aquelas que combinarem tecnologia visionária, a preço competitivo, com reforço em relacionamento construído com base em confiança e profundo entendimento nas necessidades dos negócios de seus clientes.

Assim, torna-se evidente a constatação da condição de que no mundo moderno há pouquíssimos processos de negócios que não tenham dependência, ou ao menos uma interface, com a ciência da tecnologia da informação e comunicação. Não poderia ser de outro modo no setor bancário, onde a informação constitui-se o único recurso realmente significativo, de maneira que, no momento atual de elevada competitividade em negócios onde a Tecnologia da Informação tem o potencial para transformar empresas e contribuir efetivamente na manutenção do crescimento sustentado de retorno aos investidores nas organizações, os mecanismos de Governança Corporativa são complementados por conceitos específicos de Governança em TI como prioridades nas empresas.

2.1 O Paradigma das Instituições Financeiras de Classe Mundial

As responsabilidades fundamentais da Governança Corporativa em Instituições Financeiras de Classe Mundial encontram-se em prover a direção estratégica e estabelecer controle sobre a execução das estratégias de negócios, as quais devem incluir uma visão estruturada dos investimentos em Tecnologia da Informação e, conseqüentemente, em Facilidades Prediais de Missão Crítica. Ao decidir os investimentos prioritários em TI, questões fundamentais, incluindo a natureza intangível de muitos dos resultados esperados, precisam ser endereçadas somente após a aplicação de técnicas do cálculo de retorno sobre o investimento (*ROI-Return on Investments*).

A Tecnologia da Informação introduz riscos que devem ser geridos em busca de sucesso do negócio, assim, o CEO e a Diretoria Executiva da Organização precisam oferecer a visão e diretrizes fundamentais com foco na iniciativa de Governança em TI para produzir uma estrutura contando com o correto nível de executivos envolvidos em comitê específico, esclarecidos quanto ao apetite para riscos da empresa e com responsabilidades bem definidas quanto ao gerenciamento de riscos mensuráveis e monitorados, visando oferecer relevante contribuição no provimento das garantias externas requeridas por dispositivos regulatórios como o Sarbanes-Oxley e o Basileia II. Ao descrever os domínios da Governança em TI podemos abordá-los sob cinco perspectivas básicas, conforme tópicos a seguir: ¹³

- ◆ **Alinhamento Estratégico** – foco na garantia de ligação entre os negócios e os planos de TI visando proporcionar o alinhamento entre as operações de TI e da Empresa;
- ◆ **Valor Agregado** – estratégia concentrada na otimização de custos e no provimento do valor intrínseco de TI;
- ◆ **Gerenciamento de Recursos** – foco na otimização dos investimentos e na gestão adequada dos recursos críticos de TI : processos, pessoas e aplicativos (informações);

- ♦ **Gestão de Riscos** - requer o tratamento de riscos em alto escalão da empresa, mediante o claro entendimento do apetite aos riscos, transparência quanto aos riscos relevantes e controle de responsabilidades na gestão de riscos da organização;
- ♦ **Indicadores de Desempenho** – implementação de uma nova estratégia para monitoração e avaliação de resultados, utilizando por exemplo, o sistema *“balanced scorecards”** como ação para se alcançar objetivos mensuráveis estrategicamente ao invés da métrica financeira convencional.

Nada acontece por acaso na busca por uma boa “Governança em TI”, cujos elementos devem ser preparados, adequadamente implementados e monitorados de acordo com as orientações da alta direção (CEO & Board) ao apreciar os riscos e as oportunidades do negócio inerentes à aquisição e desenvolvimento das soluções de TI na Organização. Portanto, o contexto atual de “Governança Corporativa” dos negócios em Instituições Financeiras de Classe Mundial encontra-se apoiado em Tecnologia da Informação e ao enfrentar o desafio de estabelecer a “Governança em TI” pode se deparar também com um novo paradigma – implantar um modelo para a “Governança em Facilities” da Organização.

A “Pirâmide de Tecnologia da Informação” descrita nas Figuras 10 e 11 a seguir, por sua vez, tem por base a Gestão Completa de Infra-estrutura e Instalações, a qual, em última análise e em plano básico, requer de organizações premidas por legislações específicas, tais como a Sarbanes-Oxley e Basiléia II, a capacidade de demonstrar rapidamente o controle efetivo do Gerenciamento de Facilidades Prediais (*“Facilities Management”*), cuja ausência de conhecimento em domínios específicos que permitam estabelecer o novo paradigma da “Governança em Facilities”, simplesmente tornarão ineficazes as cinco dimensões tratadas nos domínios da “Governança em TI”. Portanto, os conceitos a serem tratados nos próximos tópicos do presente trabalho, alinhando-se às idéias de “Governança Corporativa” e “Governança em TI”, vislumbram a Governança em *Facilities* como um novo

* *Balanced Scorecard* – ferramenta para a construção de um sistema de gestão estratégica.

paradigma a ser abordado por Instituições Financeiras de Classe Mundial, principalmente em ambientes críticos de *Data Centers* conforme ilustração que consta do Anexo “A”.

Figura 10 – A Estrutura de TI nas Empresas

Fonte : AUTOR

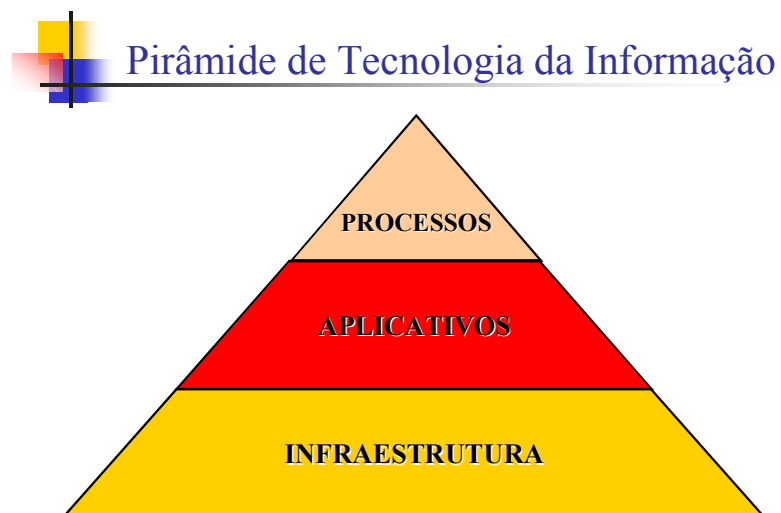
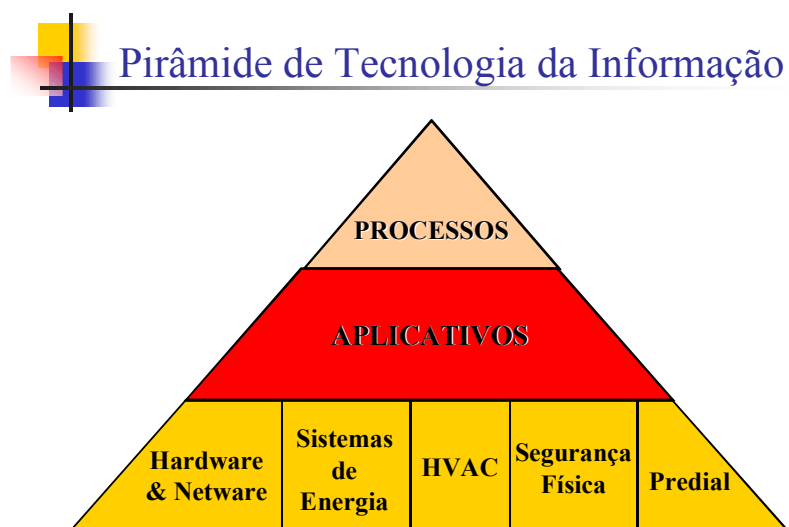


Figura 11 – Elementos de Camadas na Estrutura de TI

Fonte : AUTOR



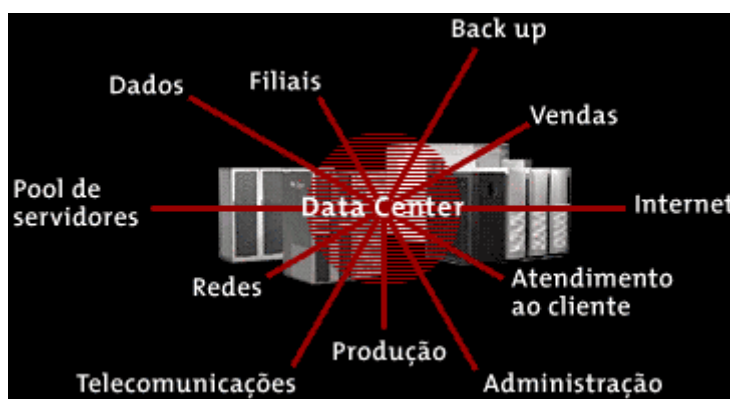
2.2 Gestão de Segurança da Informação

A gestão e o controle dos sistemas de Tecnologia da Informação (TI) visam inibir ou minimizar os riscos identificados, bem como priorizar a proteção do que é mais crítico, uma vez desenvolvidas todas as ponderações de vulnerabilidades para a configuração dos riscos, em alinhamento às diretrizes de Governança em TI conforme pode ser demonstrado no modelo COBIT que consta do Anexo “B” do presente trabalho. A etimologia do termo “risco” tem sua origem incerta e muito antiga, incorporando conceitos que passam da “fatalidade” à “fortuna” já no século XII até a expressão “risco” aplicada no século XVI. Sabe-se que o termo teve um emprego bem definido, ligado às transações comerciais no direito marítimo, embora passasse a ser usado de forma rara e numa variedade de contextos, havendo registros da palavra em português (século XV), no francês (século XVI), na antiga Mesopotâmia (finalidade mercantil nos contratos de navegação), no Egito (ocupação árabe) e na Itália como expressão própria do jogo (com o sentido de arriscar ou ousar). Em resumo, desde sua origem o termo risco foi aplicado para empreendimentos de grande monta e de contexto incerto para o sucesso, especialmente aplicado na relação mercantil com o objetivo de ratear prejuízos e benefícios.¹⁴

Na era moderna risco tornou-se sinônimo de “perigo”, criando-se a partir da segunda metade do século XX o que se passou a chamar de a “era da incerteza” com o fim da “cultura de segurança” praticada até o início do século XX. A evolução da ciência trouxe força às proposições que enfatizavam o contexto, onde diferentes aspectos ou “fatores de riscos” estariam contribuindo para o fenômeno em estudo. Nos dias de hoje o conceito de “risco” alcança praticamente todas as dimensões da vida, passando pelas ciências sociais com registro de elevado número de citações, na literatura médica cuja cifra de referências é estrondosa e no poder que agora se estabelece formalizando diretrizes de “prudência” para condicionar os desejos como uma nova forma de controle social cujo conceito já alcança até a criminologia.¹⁴

A gestão de segurança da informação ao analisar e ponderar os riscos dos ambientes físicos do *Data Center*, considera o espaço construído funcionando como um sistema e seus elementos são partes integrantes de todo um complexo de infra-estrutura física que possui a função de abrigar e proteger os ativos de TI, assim, as análises recorrem ao entendimento deste como um todo indissolúvel, cujos subsistemas possuem características funcionais específicas conforme consta do Anexo “C” do presente trabalho. A teoria de sistemas teve sua origem histórica nos Sumérios da Mesopotâmia, com a criação de um calendário para dominar o tempo, deste ponto de partida foi criada tanto a astrologia, como os sistemas de numeração decimal/hexadecimal e, ao se analisar as fases da lua, criou-se uma correspondência de ordem lógica e previsível, ou seja, um sistema. Tal teoria formalizou-se a partir dos anos 40 com a participação dos EUA na guerra mundial e vai até os dias atuais nas diferentes propostas para elaboração de software e também na composição de um ambiente físico seguro para armazenar e processar dados, ou seja, o sistema denominado de “Ambiente Físico de Missão Crítica”.¹⁵

Figura 12 – Composição Básica de TI no Data Center
Fonte : ACECOTI



Entende-se o sistema como uma forma lógica de se descrever um conjunto de elementos que permite a percepção de uma condição de ordem e a proposição de uma forma operativa voltada para um dado objetivo, ou seja, pode-se definir o sistema como uma coleção de entidades, relacionadas ou conectadas de tal modo que formam um todo. O Data Center, como sistema descrito na Figura 12 acima, possui

diversos elementos ou entidades (pessoas, máquinas, objetos, informações e subsistemas) que interagem num meio ambiente (interno ou externo) e dispõe de uma organização própria, compreendendo relações em uma estrutura e um processo de funcionamento.

O ambiente físico de *datacenter* deve considerar que o potencial de riscos a ser levado em conta na busca da disponibilidade otimizada dos dados e de sistemas é multifacetado. É indispensável o levantamento e avaliação de cada um dos riscos, mas a avaliação só é possível após o exame conjunto de todos os componentes de risco. A avaliação do potencial específico de risco depende necessariamente da probabilidade de ocorrência de um dado evento, e esta por sua vez depende de muitos fatores individuais existentes na área ao redor do CPD e dos sistemas de hardware, conforme apresentado na Figura 13 a seguir.

Figura 13 – Ameaças ao Ambiente Físico

Fonte : ACECOTI

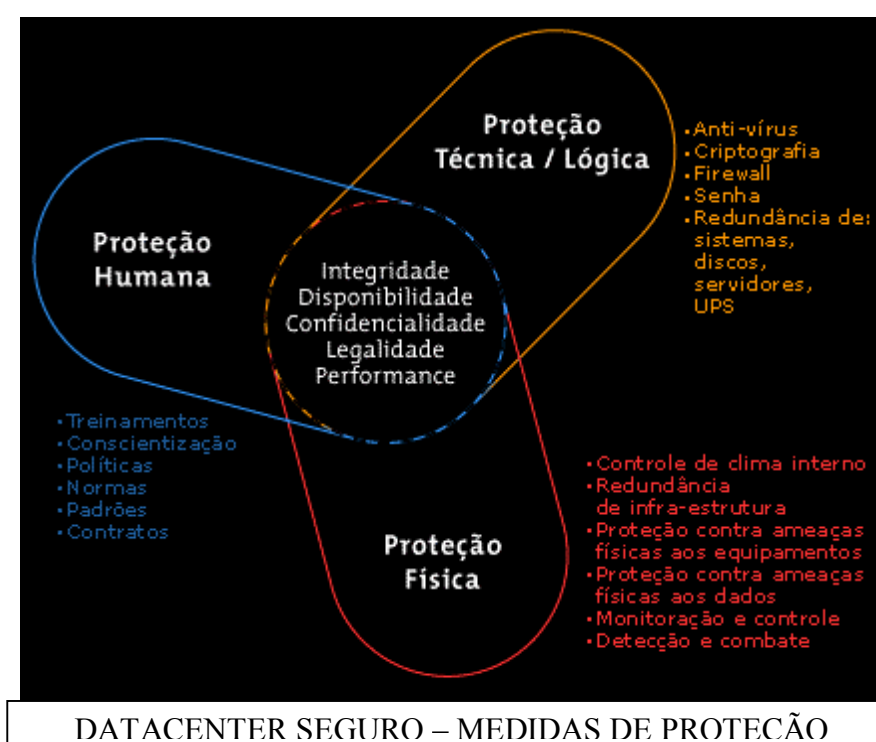


Exames analíticos e a avaliação de muitos sinistros diferentes mostram um cenário de ameaças que pode ser ponderado da seguinte maneira : riscos relacionados com pessoas (colaboradores internos); riscos de catástrofes naturais (força maior); riscos de paralisações dos sistemas (downtime); riscos de influências criminosas externas (ataques). A qualidade do ambiente físico é fundamental para a disponibilidade dos sistemas de informações e envolve seis pontos básicos, a saber : proteção contra sinistros naturais, acidentais e intencionais; alimentação ininterrupta de energia; suprimento contínuo de ar climatizado-refrigeração; acesso seguro e controlado das

peças e equipamentos; monitoração e organização preparada para emergências; adaptabilidade às reconfigurações futuras. As medidas de proteções que buscam proporcionar no *datacenter* os resultados esperados de disponibilidade, integridade, confidencialidade, legalidade e performance, concentram-se conforme disposto na Figura 14 a seguir.

Figura 14 – Medidas de Proteção em *Data Center*

Fonte : ACECOTI



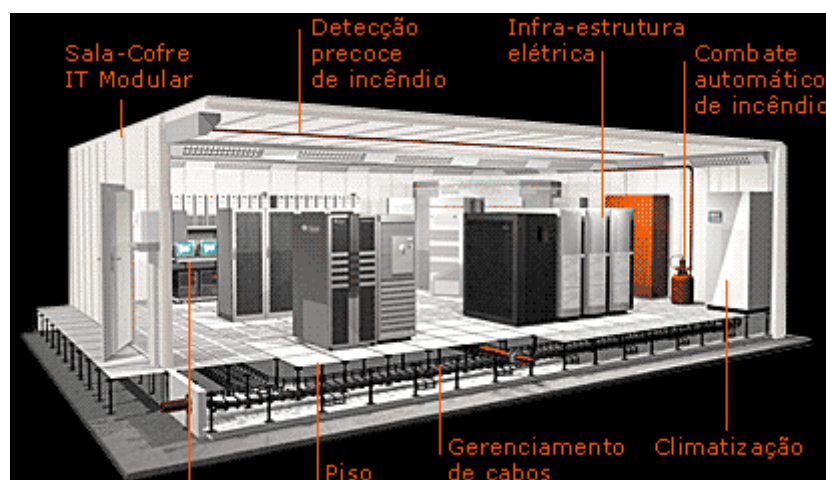
A concepção dos conceitos de *Datacenter* Seguro e Inviolável, aplicados às condições intrínsecas do local escolhido, buscam na flexibilidade uma qualidade fundamental do projeto, visto que soluções flexíveis facilitam mudanças, portanto, também reduzem os riscos inerentes em alterações nos ambientes físicos e sua infra-estrutura. A evolução e a demanda por áreas cada vez mais seguras e confiáveis para a Tecnologia da Informação tem aumentado e os clientes de TI esperam confiabilidade e disponibilidade elevadas no *datacenter*, além da possibilidade de se executar atividades de manutenção planejada de infra-estrutura sem desligar a carga crítica e ser simultaneamente mantido. É importante lembrar que um *datacenter*

típico é composto de pelo menos 20 (vinte) principais itens nas áreas mecânica, elétrica, proteção contra fogo, automação predial, supervisão, segurança e outros sistemas, cada um deles com subsistemas adicionais e seus componentes, bem como, a qualidade no gerenciamento dos fatores humanos é um dos elementos mais significantes e devem ser tratados nas definições dos procedimentos de operação, manutenção e monitoração, como um conjunto de funções e responsabilidades do Gerenciamento de Facilidades que pode ser descrito conforme consta do Anexo “D” do presente trabalho.

A conceituação para o ambiente datacenter prefere entender os “fatores de riscos” como sendo as características ou circunstâncias cuja presença está associada a um aumento da probabilidade de que o dano venha a ocorrer e o resultado de todo o esforço investigativo acaba se convertendo num marco de fronteira entre o seguro e o perigoso, logo, a redução do risco intrínseco (no ambiente) implica diretamente em redução das perdas por acidentes. A exclusão da incerteza é uma forma de uso do conhecimento científico que se presta à exclusão do acaso e da tragédia e seu propósito é promover o mito do sistema sem espaço para qualquer não conformidade, servindo-se do logro através do esplendor sistêmico que permite o paradoxo da retomada de relações de causa-efeito no âmbito do conceito de “risco”.

Figura 15 – Exemplo de CPD em Sala Cofre

Fonte : ACECOTI



De modo que o CPD possua as características de um verdadeiro cofre como no exemplo que consta da Figura 15 na página anterior, como construir um datacenter seguro ? A gestão de riscos no *datacenter* deve considerar todas as questões visando identificar as “ameaças” ou “fatores de riscos” à Tecnologia da Informação. Assim deve ser preparada para oferecer soluções e responder aos diversos questionamentos, tais como : a corporação pode sobreviver sem informações ? a perda de informações paralisa a empresa ? as corporações estão cada vez mais dependentes da tecnologia da informação ? o volume de dados armazenados cresce a cada dia ?

A fragilidade e a suscetibilidade dos sistemas, constantemente sob ameaças físicas (incêndios, impactos, gases corrosivos, radiações, magnetismo, poeira, alagamento), ameaças tecnológicas (panes de hardware, falhas de energia elétrica, falhas de climatização, vírus, cavalos de tróia, vermes eletrônicos, bombas lógicas, hackers, acessos indevidos aos sistemas, falhas de software) e ameaças humanas (negligência, erros de operação, fraudes, vandalismo, sabotagem), torna as corporações vulneráveis a paradas de operação por acidentes, cujas ocorrências podem significar prejuízos irreversíveis comprometendo a continuidade dos negócios.

O amplo “quadro de ameaças” ou “fatores de riscos” precisa ser devidamente tratado através de medidas apropriadas de proteção que visam proporcionar ao *datacenter* os resultados esperados de disponibilidade, integridade, confidencialidade, legalidade e performance. Assim todo evento fortuito que possa causar paralisação, falha de operação ou perda de informação do cliente deve ser objeto de enfoque nos sistemas de segurança do *datacenter*, tendo como função de monitorar, controlar e impedir a ocorrência deste através da implantação de dispositivos para o controle de acesso, detecção de intrusão, monitoração de imagens, sistemas antifurto, detecção precoce e pontual de incêndio, extinção de incêndios, detecção de líquidos/vapores, interferências eletromagnéticas, proteção contra descargas atmosféricas, todos estes interligados à um sistema de supervisão e inteligência predial, possibilitando o monitoramento de parâmetros essenciais e acionando alarmes em caso de desvios ou eventos que possam colocar em risco a segurança ou operação do CPD.

Obviamente que antes de qualquer ação sobre os “fatores de riscos” nas instalações de *datacenter*, eles devem ser objeto de estudos e análises para que sejam conhecidos e classificados, sendo que a gestão de riscos deve se aprofundar nas operações da organização e descobrir efetivamente os riscos expostos. Alguns riscos são relativamente de fácil identificação e outros podem não ser identificados numa visão geral, mas há importantes ferramentas de aproximação ao problema de identificação de riscos que incluem *check-lists* da política de seguros, questionários de análise de riscos, quadros do fluxo de processos, análises de dados financeiros e inspeções em campo das operações da organização.

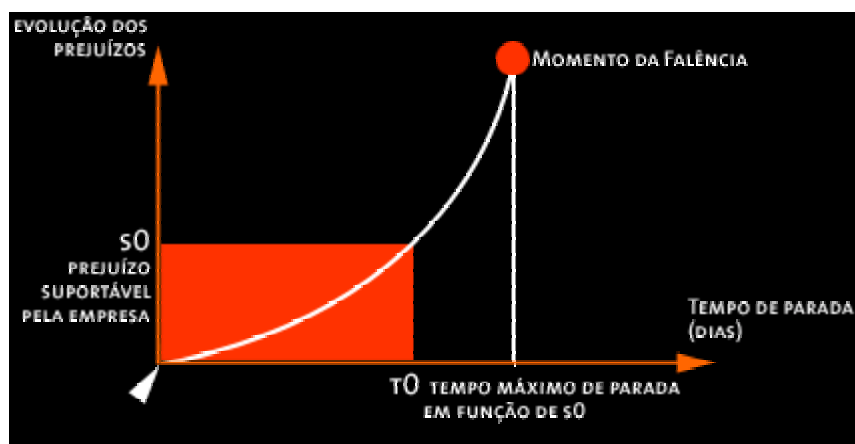
A avaliação quantitativa nos permite a identificação-reconhecimento dos riscos (“a priori”) com a aplicação específica de conceitos e técnicas aos sistemas sob análise (homeostase, árvores-descrição do processo/ “*what if*”, *checklists-walk trough*/prioridades/matriz de exposição), bem como nos permite a investigação de eventuais acidentes com aplicação também específica de teorias (mono-multicausal, risco/acaso-complexidade) e técnicas (simulação-árvores, causa-efeito/espinha de peixe, AF/Boing, matriz hierárquica, “*TOR-Technic of Operations Review*”).¹⁴

Qualitativamente podemos analisar vários aspectos do funcionamento do *datacenter* efetuando vários questionamentos e identificando as premissas dos negócios, tais como: Quanto tempo a empresa suportaria a parada do seu *datacenter* ? Qual é o custo de parar e de se recuperar ? Qual o impacto desta interrupção ? Qual o nível do investimento necessário e a proteção mais adequada ? Qual o acordo do nível de serviços com seus clientes internos e externos ? Qual a disponibilidade desejada pela empresa ? 99,9% ? É possível tolerar 8 horas/ano de paralisação que corresponde ao 0,1% de tolerância ? Quanto tempo a empresa leva para recuperar a performance após um acidente ? Discos - quanto tempo para recuperar informações on-line? Back-ups - qual o tempo para recuperação dos back-ups ? eles estão 100% atualizados ? Equipamentos - qual o tempo dos fornecedores para repor Telecom (*switchs, routers*, controladores, dentre outros), Servidores, Mainframes, Robots, Nós de Redes ? Sites de Contingência – os processos críticos estão identificados ? Existe um site alternativo para os processos críticos e ele está 100% preparado para atender aos seus acordos de níveis de serviço? Quanto tempo para relocar equipamentos e

peçoal ? Qual o momento que, a partir dele, a sobrevivência de uma empresa corre perigo com a parada do processamento ? Todas estas questões podem contribuir para se determinar o tempo máximo de sobrevivência de uma empresa a partir da interrupção dos serviços de processamento de dados, conforme a ilustração gráfica que consta da Figura 16 a seguir.

Figura 16 – Momento de Falência em Parada do CPD

Fonte : LOSS CONTROL



Podemos ainda nas análises qualitativas identificar os diversos fatores de riscos físicos através de inspeções em campo das instalações e operações do *datacenter* e identificar focos de problemas. O progresso tecnológico demanda riscos, a atividade diária demanda riscos, a própria vida demanda riscos e a capacidade de utilizarmos todos os recursos disponíveis para a eliminação ou redução desses riscos configura um princípio a ser perseguido e os resultados são de amplo alcance, tanto para os empresários que garantem um dimensionamento adequado de seus riscos e a prevenção apropriada, quanto para o mercado segurador como um todo (seguradores, resseguradores e corretores) que dispõem de subsídios e técnicas de análise cada vez mais aperfeiçoadas, consolidando a seriedade e credibilidade inerentes a esse trabalho, implicando em benefícios que são de todos em face do desenvolvimento e manutenção de negócios.¹⁶

A gestão de segurança da informação possui um aspecto de maior ênfase nas ações preventivas descritas pela gestão de riscos, mas também não deve prescindir de

analisar todas as ações necessárias no caso de ocorrência de algum desastre, catástrofe ou mesmo qualquer contingência de funcionamento nos ativos de TI e Telecom que são mantidos no ambiente físico do CPD, sendo este o enfoque da gestão de crises. A etimologia da palavra crise tem sua origem no latim significando “momento de decisão, mudança súbita” e no grego como “ação ou faculdade de distinguir-decisão-momento decisivo”, cujo conceito possui diferentes dimensões de caráter individual ou coletivo e pressupõe a idéia dos deflagradores com base em fatores de riscos e características anunciadas. A crise possui causa e contexto e decorre como consequência do risco ou incertezas, trazendo implicações para o edifício no território de suas relações e no âmbito de responsabilidades da gestão e entidades envolvidas. A gestão de crises ou gestão de emergência visa planejar e estabelecer responsabilidades antes, durante e depois de ocorrida a crise, definindo as ações do pessoal especializado (ex: bombeiros) ou não especializado (ex: escritório). A gestão de emergência tem por objetivo desenvolver e manter um programa de emergência, o qual deve definir e avaliar os perigos potenciais, estimar os recursos necessários para atender emergências, manter inventário e determinar necessidades não atendidas, fazer plano de contingência, adequar periodicamente e estabelecer as mudanças deste programa.¹⁷

A gestão de crises ou de emergências no *datacenter* remete-nos ao conceito de contingência que nos leva a pensar no fato de o serviço, do departamento ou da empresa não poder parar se determinados problemas ocorrerem. São muitos os exemplos de responsáveis previdentes que pensam e buscam implementar as contingências necessárias para caso ocorra um problema grave com equipamentos, sistemas, pessoal e serviços básicos, ou seja, com qualquer fator que possa ser considerado essencial para a manutenção das informações críticas e continuidade dos processos sob sua responsabilidade, sendo esta uma característica desejável, pois beneficia a organização e conseqüentemente a seus clientes internos e externos. Se é comum encontrar tais situações, porque o processo de gestão de crises deve nos levar a pensar em desenvolver um Plano de Contingência para o *Data Center* ?

Dentre várias respostas possíveis, duas se destacam para justificar este plano :

- Um problema ou desastre que inviabilize a continuidade de um processo fundamental para a organização pode ocorrer de maneira imprevisível e ela pode não estar preparada para uma saída rápida e eficaz do problema;
- Ainda que exista uma solução adequada, nem todos os que devem ser acionados saberão agir de forma ordenada ou poderão ser localizados e isto pode aumentar em muito o tempo de ativação da contingência, agravando a situação e afetando os clientes.

O que diferencia um bom Plano de Contingência são os resultados alcançados que ocorrem em função da participação adequada das pessoas-chave responsáveis pelas operações e das técnicas utilizadas nas várias análises que precisam ser feitas – valores, riscos, impacto, criticidade, desastre, estratégias, tática – baseadas em levantamentos, entrevistas na infra-estrutura, investimentos disponíveis, processos, sistemas e condições básicas como back-up. Tudo deve ser feito numa sequência logicamente. Como exemplo, nas análises de riscos de um determinado processo são identificados os fatores críticos de que este depende, qual o grau de dependência e a respectiva confiabilidade. O resultado destas análises consiste no que é essencial no plano – são definidas as melhores estratégias de contingência e as atividades a executar em cada possível desastre contemplado para toda a equipe envolvida. Assim, ao se pensar em desenvolver um Plano de Contingência para o *datacenter* podem ocorrer vários questionamentos de diversas ordens e até mesmo pode ser considerado um conceito de site de contingência que se constitui num outro ambiente físico totalmente preparado para obedecer os seguintes requisitos :¹⁸

- Site preparado para assumir toda a produção em caso de contingência;
- Ambiente inviolável e seguro como o site principal;
- Preservar a continuidade de negócios da organização.

O crescimento na adoção de tecnologias da informação nas instituições, o cenário de globalização da economia com as informações assumindo papel estratégico nas negociações e afim de responder às mais diversas necessidades, os órgãos reguladores e as empresas de auditoria independentes, bem como os vários parceiros

de negócios e muitos deles internacionais, têm exigido que as empresas evidenciem as medidas tomadas para garantir a integridade e disponibilidade dos dados necessários para a concretização de transações de toda ordem, utilizando-se como base as mais variadas normas desde o segmento financeiro com os acordos de Basiléia/Basiléia II e circulares do Banco Central (CI 2892), bem como das mais atualizadas normatizações técnicas de segurança da informação, destacando-se a NB-1334 e NB 1335 que fixam as condições ambientais exigíveis para cada mídia de armazenamento de dados, além das ISO 27001:2005, NBR ISO/IEC 17799:2005 e a Euronorma EN 1047:2 que discorrem de maneira geral e abrangente sobre as diretrizes para os ambientes de CPD.¹⁹

Ao elencar os principais requisitos de segurança física com ênfase na Gestão de Riscos em ambiente *Datacenter*, consideramos as melhores práticas a serem aplicadas nas instalações deste tipo de ambiente em edificação de Missão Crítica, mediante o desenvolvimento da aplicação teórica para dar conta de acontecimentos com o uso da Teoria Geral de Sistemas, o Conceito de Risco, das teorias e técnicas para identificação de perigos nas Avaliação Quantitativa, das configurações de valores de probabilidade e implicações da modelagem na Avaliação Qualitativa, das ponderações de Vulnerabilidades, das possibilidades de superação dos problemas pelos Controles, das abordagens de aspectos extra-técnicos na metodologia de Gestão e a classificação de critérios nas medidas de tratamento de Crises na Gestão de Emergências.

Um plano de verificações de vulnerabilidades físicas deve ser moldado para analisar cada problema em potencial e cada um de seus impactos, consequências e efeitos, os quais devem ser considerados sob três perspectivas de tempo – antes, durante e depois do incidente. O ponto mais importante ao se preparar um *check-list* de vulnerabilidades é de que se possa incluir todos os espaços do edifício – espaço de uso específico, espaços comuns, sistemas de suporte, espaços de infra-estrutura, enfim, todo e qualquer espaço aberto, seja no telhado ou em subsolos, corredores, halls e garagens.

Em cada um dos itens que constam do *check-list* o analista deve indicar o que descobriu, utilizando-se de quatro categorias para classificação : (1) atenção imediata; (2) problema potencial; (3) aceitável; (4) não se aplica. A metodologia de pesquisa deve prever que os levantamentos ocorram de fora para dentro do ambiente sob análise, ou seja, os aspectos do exterior do prédio devem ser considerados em primeiro plano, seguindo-se para a entrada, recepção, áreas comuns localizadas no andar térreo, posteriormente, as áreas de coberturas com a observação de estruturas ali posicionadas, tais como as torres de resfriamento, reservatórios de água, helipontos e aspectos do telhado. A pesquisa deve se estender para os andares abaixo incluindo-se os andares em subsolos com as casas de máquinas, almoxarifados, passagens de leitos e cabeamentos elétrico e de telefonia, bem como tudo mais que possa estar posicionado de cima até embaixo no edifício.²⁰

Em todos os andares e espaços considerados se faz de vital importância a inspeção do que está atrás daquelas “portas misteriosas” que ninguém parece conhecer ou saber quem tem as chaves, bem como, quaisquer outros itens que não estejam presentes no check-list básico que deve ser desenvolvido para cada prédio envolvido nas análises de impacto aos negócios da organização, cujos quesitos podem ser considerados para as condições associadas nas categorias de ambientes relacionados, conforme segue :

- i. Localização e implantação do Site;
- ii. Aspectos Gerais do Edifício : condições gerais, gerenciamento, recepção e acesso, cobertura, elevadores, saídas de emergência, sobpisos e entreforros, salas de arquivos, salas de computadores e telecomunicações, escritórios, equipamentos e serviços de telefonia, corredores de circulação, ambientes de apoio (sanitários/copa/cozinha/cafeteria/ambulatório/escadarias/dentre outros);
- iii. Equipamentos e serviços elétricos : geradores de emergência, painéis e quadros de força, UPS, salas de baterias, gerenciamento de energia, subestações, passagens de cabeamentos;
- iv. Ar-condicionado : casas de máquinas, sistema de tubulações hidráulicas, salas de fancoils, dutos e plenos de distribuição de ar;

- v. Sistemas de Segurança, Detecção e Alarmes, Combate à Incêndios : controle de acessos, alarmes de fumaça, proteções contra incêndios, proteção contra intrusão, sistemas de combate via sprinkler ou gases, detectores de líquidos, dentre outros;

Um problema em potencial existe quando o item ou condição considerada resulta em danos às pessoas ou risco de vida, danos ao espaço físico ou interrupção de processos críticos, sendo que, o processo de análises via o *check-list* de vulnerabilidades físicas deve endereçar quais são os riscos, o nível de impactos e consequências, além de seus efeitos, visando reduzir tais riscos ao nível de *ALARP-As Low as Reasonable Practicable* (Tão Baixo Quanto Razoavelmente Praticável). A metodologia de pesquisa de vulnerabilidades físicas pode considerar vários itens nas listas de quesitos a serem aplicados aos ambientes sob análises, cuja plenitude e abrangência do plano deve ser desenhado em cada caso concreto para servir de modelo ou referência ao desenvolvimento de um *check-list* específico.²⁰

Neste sentido, além de prover uma visão geral de vulnerabilidades físicas que devem ser consideradas nas planilhas de *check-list* dos quesitos para coleta de informações sobre os ambientes de Missão Crítica para TI em Instituições Financeiras de Classe Mundial, também deve ser elencado o nível aceitável de risco que a empresa pode conviver, ou seja, considerando-se tudo aquilo pode ser “aceitável” ou “tolerado” na totalidade de riscos concernentes às pessoas, espaços e processos que venham implicar em “salvaguardas” aos resultados operacionais da Organização.²¹

Muitas organizações já estão começando a entender que uma boa estrutura de gerenciamento de segurança da informação pode ser um fator tão crítico para o sucesso e continuidade de um negócio quanto a estrutura do gerenciamento de TI . Para se criar tal estrutura de gerenciamento de segurança da informação, as melhores e boas práticas podem ser consideradas em um escopo básico de providências, conforme o exemplo relacionado no conjunto de atividades descritas nas proposições como segue : ¹⁹

- Antes de mais nada, deve ser criada uma estrutura organizacional para iniciar, implementar e controlar a segurança da informação dentro da empresa. Dois fatores são essenciais : o comprometimento/suporte da alta administração e a indicação de responsável pelo gerenciamento da segurança;
- Um Comitê de Gerenciamento deve ser criado para promover a segurança da informação dentro da organização através do comprometimento e recursos necessários para a implementação. O comitê deve tratar dos seguintes pontos : revisão e aprovação da política de segurança da informação; monitoramento da exposição dos ativos de informação às ameaças; revisão e acompanhamento dos incidentes de segurança; aprovação de iniciativas para melhorar a segurança da informação;
- Um Gestor de Segurança da Informação deve ser nomeado para arcar com toda a responsabilidade pelo desenvolvimento, implementação da segurança e pelo suporte à identificação dos controles. Além disso, as responsabilidades individuais pela proteção dos ativos e condução dos processos específicos de segurança devem ser claramente definidas;
- Várias responsabilidades podem ser delegadas a outros colaboradores ou prestadores de serviços, mas uma pessoa tem que ser a responsável final, sendo capaz de demonstrar que toda responsabilidade delegada está corretamente mantida;
- Um processo de autorização para novas aquisições de tecnologia da informação deve ser estabelecido. Estes controles são especialmente importantes em ambiente de rede;
- Consultores de segurança da informação, internos ou externos, devem ser procurados e contratados. A qualidade das análises e avaliações das ameaças à segurança e as recomendações de controles são os que determinarão a eficiência da segurança da informação na organização;
- Contatos legais com autoridades, instituições reguladoras, provedores de serviços de informação e operadores de telecomunicações deverão ser mantidos de forma a garantir que rapidamente possam ser tomadas ações e obtidas as recomendações, na ocorrência de incidentes de segurança;

- A implementação da segurança da informação deve ser revisada independentemente (auditoria interna ou consultoria especializada) para oferecer garantia de que as práticas da organização refletem apropriadamente a política adequada e eficiente.

2.3 Conceitos em Facilidades Prediais de Missão Crítica

A cada ano podemos verificar uma situação muito comum à muitas pessoas em escolas, escritórios, vizinhanças e outros tantos lugares, quando, principalmente nas mudanças de estações, começam a sentir dores no corpo e cabeça, coriza, mau-estar e outros sintomas daquele desconfortável incômodo – a gripe. O que fazer nesta situação? A maioria procura a farmácia mais próxima em busca de um antigripal qualquer, quando muito, em páginas amarelas ou listas de referências procuram por um médico clínico geral. Entretanto, se o mesmo caso acontecer ao filho único de um casal, acompanhado de forte dor de ouvido, com certeza, o médico da família será chamado ou um pediatra de confiança ou, até mesmo, um médico de grande especialização como um “otorrinolaringologista” e, não raro, será aquele profissional recomendado por vários amigos e familiares.

Eis a razão porque cercar-se de “especialistas” – há uma necessidade de se tratar um “caso especial”, onde as circunstâncias e os riscos associados requerem profissionais extremamente preparados, focados em áreas específicas do conhecimento, ou seja, pessoas que conhecem muito bem os riscos e como minimizá-los – assim, isto tanto é verdade nas profissões médicas ou jurídicas, na qualidade de *serviços personalíssimos e revolucionários para mudar as regras do jogo*²², como no campo do *design* presente na arquitetura, engenharia e construção dos Prédios de Missão Crítica, a exemplo daqueles que abrigam soluções de Tecnologia da Informação em Instituições Financeiras de Classe Mundial.

O que faz do MCF-*Mission Critical Facilities* (Facilidades de Missão Crítica) uma especialidade ? De início, a operação de negócios relacionada requer um profundo entendimento dos requisitos e elementos da Tecnologia da Informação (TI) – roteadores, servidores, mainframes, redes LAN/WAN, discos, robôs, etc – e das condições necessárias para manter estes equipamentos funcionando adequadamente.

A história do seguimento de MCF-*Mission Critical Facilities* está associada à história da Tecnologia da Informação que a partir do começo dos anos 70 passou a estar em destaque com o lançamento dos computadores de grande porte, os chamados *mainframes* usados para uma variedade de aplicações matemáticas, cujos conceitos foram entrando, infiltrando-se e sobrepondo-se aos negócios no mundo, até chegarem ao contexto atual de completa dependência de “TI & *Facilities*” como o evidenciado nas Instituições Financeiras de Classe Mundial. A aceleração do avanço tecnológico no último século é impressionante como se pode verificar através da análise de velocidades do fluxo de informações, demonstrado na Tabela 1 a seguir, cujo encurtamento crescente do tempo verificado entre o aparecimento de novas invenções pode ser atribuído aos ciclos virtuosos criados por um avanço científico que possibilita outros e assim sucessivamente, bem como, por uma velocidade de propagação de informações decorrente dos avanços sucessivos, as quais alcançam cada vez mais pessoas cada vez mais rápido.²³

Tabela 1 – Velocidade de Propagação das Informações

Fonte: ZUFFO (1997)

Era	Duração (anos)	Velocidade de Interação (km/h)
Primitiva	20.000 – 40.000	0,4 – 0,8
Agro-pastoril	2.000 – 4.000	4 – 8
Industrial	200 – 400	40 – 80
Pós-industrial	20 – 40	400 – 800
Infoera	2 – 4	4.000 – 8.000

Apesar de comparado à um elefante no tamanho, o primeiro *mainframe* era frágil quanto aos requisitos ambientais para o seu funcionamento e produzia calor suficiente ao disparo de três estágios do alarme de incêndio. As empresas dispostas a manter este tipo de “brutamontes” em operação, precisavam construir salas especialmente preparadas com sistemas de ar-condicionado e ventilação, sendo este fato a primeira interseção histórica da Tecnologia da Informação com a Engenharia/Arquitetura. Ainda nos anos 70 os “mainframes” começaram a serem substituídos por computadores muito menores – o PC (“*Personal Computer*”) – e as empresas começaram a confiar as suas informações financeiras e processamento de dados à estas máquinas.²⁴

Na medida em que a indústria digital progredia rapidamente, as organizações começaram a ficar extremamente vulneráveis às falhas dos computadores, entretanto, tão logo quanto este problema foi evidenciado a indústria digital passou a construir equipamentos de melhor qualidade, superando a marca dos 99% de confiabilidade. Este constituiu-se o grande marco histórico para o nascimento do MCF-*Mission Critical Facilities*, quando as instalações prediais que abrigavam os computadores começaram a falhar mais do que os equipamentos de TI por suas causas próprias, onde começaram a ficar evidentes as falhas de energia essencial e os problemas de ar-condicionado, bem como os requisitos de TI por melhorias de qualidade dos sistemas de infra-estrutura básica, ou seja, nascia a necessidade do MCFM-*Mission Critical Facilities Management* (Gerenciamento de Facilidades de Missão Crítica) com os seus três requisitos essenciais ou desafios principais de elevação do desempenho nos sistemas – Disponibilidade, Confiabilidade e Flexibilidade de Manutenção (Manutenibilidade).

Afinal de contas, o que é a área de MCF-*Mission Critical Facilities* ? A maneira mais fácil de explicar esta especialidade que requer abrangência multidisciplinar do conhecimento (engenharia, arquitetura, legislações, TI, administração e outros complementares) pode ser encontrada ao se dissecar a própria composição do termo, como segue : ²⁵

- ◆ ***Mission Critical (Missão Crítica)*** – se refere à tecnologia que suporta um negócio essencial ou função governamental de caráter funcional ininterrupto (operação: 24horas/dia e 365 dias/ano). Isto engloba qualquer parte do sistema crítico de equipamentos – se alguma destas apresenta falhas pode implicar em perdas significativas para a empresa, seus funcionários, seus investidores ou sua reputação;
- ◆ ***Facility (Facilidade ou Instalação)*** – se refere ao prédio, estrutura ou infraestrutura, edifício, instalações, facilidades prediais ou qualquer outro sinônimo que se possa encontrar no dicionário;
- ◆ ***Mission Critical Facility (Facilidade de Missão Crítica)*** – se refere ao sistema predial como um todo ou seus subsistemas internos em específico que abrigam e/ou suportam os computadores e seus equipamentos auxiliares de TI. Tradicionalmente há três elementos fundamentais na composição típica dos Prédios de Missão Crítica, a saber:
 - “*The Data Center*” (CPD-Centro de Processamento de Dados), um repositório central de computadores e outros equipamentos auxiliares de TI que gerenciam as aplicações críticas da empresa;
 - “*The NOC-Network Operation Center or The SOC-Security Operation Center or CC-Comand Center*” (Centro de Controle Operacional e de Segurança da Rede de Computadores), uma sala especialmente desenhada para alocar os recursos (humanos e físicos) visando a monitoração e operação dos equipamentos de TI do CPD. Esta é a área onde os funcionários da empresa supervisionam as atividades dos sistemas de TI – *mainframe*, discos, servidores, *firewall*, tráfego de Internet, desempenho dos circuitos de comunicações de dados, capacidade de armazenamento de dados, invasão dos sistemas de informação, distribuição de software e atividades relacionadas.
 - “*The Energy Plant*” (A Fonte Principal de Infra-estrutura Básica ou Planta de Energia), um conjunto de áreas específicas de infra-estrutura básica do Prédio de Missão Crítica, onde concentram-se as fontes essenciais de energia (geradores, UPS/No-break, baterias, painéis principais de força, transformadores, chaves estáticas, chaves de transferências e outros) e de

climatização ou ar-condicionado (refrigeração/ventilação/aquecimento: chillers, centrífugas, fancoils, bombas, torres de arrefecimento, tubulações hidráulicas, válvulas e outros);

- ♦ ***Mission Critical Facilities Management* (Gerenciamento de Facilidades de Missão Crítica)** – se refere ao processo de gestão dos ativos físicos da infraestrutura básica de instalações prediais em um sistema de Missão Crítica, com a função de abrigar e suportar computadores e demais equipamentos de TI. Trata-se de especialidade técnica no ramo do Gerenciamento de Facilidades que também envolve um conhecimento de maior abrangência multidisciplinar (administração, “*TI & Facilities*”, legislações, engenharia de valores, gestão de riscos operacionais, governança, segurança física, dentre outros), visando produzir a **Interação PPP** (Pessoas, Processos e Propriedades) para alcance dos objetivos estratégicos da atividade-fim de Tecnologia da Informação e suporte aos negócios da Organização.

O Gerenciamento de Facilidades de Missão Crítica (*Mission Critical Facilities Management*), em última análise, trata-se do modelo proposto visando produzir uma Gestão Completa de Infra-estrutura e Instalações, cuja estratégia principal encontra-se fundamentada no conceito de que missão crítica significa funcionamento ininterrupto 24 horas/dia, 07 dias/semana, 365 dias/ano e, até mesmo, 366 dias/ano- bissexto, ou seja, a busca da máxima disponibilidade dos sistemas de infra-estrutura básica que, na atualidade, constitui-se em manter quase cinco nos índices percentuais envolvidos (99,999% ou próximo disso, com os índices da ordem de 99,995% alcançados na mais alta categoria definida para os CPD's de Classe Mundial – a Classe IV).

Assim, nasce o conceito básico, que neste trabalho foi denominado de “Governança em *Facilities*”, focado na necessidade de uma estratégia visando produzir maior confiabilidade aos sistemas de infra-estrutura básica, efetivo controle dos ativos físicos e capacidade de agilizar os demonstrativos de desempenho na gestão completa dos recursos envolvidos em processos alvos das verificações de *Performance & Compliance* por auditorias internas ou independentes. Tal

estratégia, pode ser descrita através de cinco tópicos básicos visando incrementar a confiabilidade e gerenciabilidade do conjunto de recursos de MCF-*Mission Critical Facilities*, a saber :

- i. **Redundância** – componentes secundários do sistema que iniciam operação instantânea ou permanecem em operação contínua, de tal modo que se o componente primário falha, o secundário supre a necessidade e não resulta em falha do sistema como um todo;
- ii. **Manutenibilidade** – habilidade para se desenvolver uma rotina de manutenção em qualquer componente da infra-estrutura básica sem afetar a missão ou o processo de funcionamento vital dos equipamentos de TI, implicando em possibilidade de cumprir o plano geral de intervenções técnicas (preventivas, preditivas ou eventuais corretivas) recomendadas pelos fabricantes dos materiais/equipamentos e por legislações/normativas vigentes;
- iii. **Flexibilidade** – habilidade para se antecipar futuras mudanças no espaço físico, comunicações, densidade de cargas nas áreas de energia e ar-condicionado, oferecendo adequada capacidade de resposta às necessidades de mudanças sem afetar as aplicações críticas de TI;
- iv. **Resistência à Catástrofe** – proteção contra forças físicas e desastres naturais que podem acontecer a qualquer tempo;
- v. **Segurança** – proteção contra falhas ou lacunas de segurança nos processos e sabotagem. Em detrimento disso, nem todos os sistemas de MCF-*Mission Critical Facilities* são projetados e construídos focados em confiabilidade e algumas empresas priorizam sobretudo os custos, sacrificando os detalhes que protegem as aplicações de Missão Crítica. Tal prática pode permitir uma operação adequada por alguns poucos anos, mas rapidamente encontra uma situação de infra-estrutura obsoleta agravada por freqüentes falhas de funcionamento dos sistemas prediais que implicam em paralisações indesejadas dos equipamentos de TI, prejuízos financeiros e detrimento de imagem da Organização.

Em resumo, podemos concluir que um Prédio de Missão Crítica possui uma estrutura sofisticada que suporta a tecnologia vital aos negócios empresariais ou operações

governamentais, desta forma, nunca poderá ser abordado como os edifícios convencionais onde os recursos de infra-estrutura são implantados com preocupações distintas daquelas presentes em aplicações com necessidades de se manter uma permanente ininterruptibilidade de operações e de corresponder às exigências dos mais elevados índices percentuais quanto aos fatores de disponibilidade, confiabilidade e manutenibilidade das instalações físicas, constituindo-se o objeto de atuação na Gestão Completa de Infra-estrutura e Instalações contido no modelo proposto neste trabalho de Governança em *Facilities* para contribuir no Gerenciamento de Facilidades de Missão Crítica (“*Mission Critical Facilities Management*”).

2.4 Classificação de CPD's (Desempenho Físico)

Uma das questões mais polêmicas no campo da ininterruptibilidade de funcionamento dos recursos de MCF-*Mission Critical Facilities* (Facilidades de Missão Crítica) constitui-se em estabelecer uma classificação de confiabilidade dos ambientes físicos de infra-estrutura básica para o suporte das funções críticas de TI e, conseqüentemente, dos negócios das empresas, assim, muitos esforços têm sido empreendidos por várias associações e institutos de classe que congregam inúmeros profissionais do Gerenciamento de Facilidades em âmbito mundial, com a finalidade de estudar os aspectos especiais relevantes deste segmento e seus casos típicos de ocorrências, bem como buscar estabelecer um padrão comum de *benchmarking* (comparação) deste mercado.

Ao estudar o desempenho físico para a classificação dos espaços construídos de CPD's se faz necessário entender alguns aspectos sobre a funcionalidade dos edifícios que está diretamente relacionada com os seus sistemas prediais, uma vez que estes são elementos integrados ao edifício, que têm por finalidade dar suporte às

atividades dos usuários, suprindo-os com os insumos necessários e fornecendo-lhes os serviços requeridos. A definição de funcionalidade adotada pela ASTM-*American Society for Testing and Materials* é: “ser adequado para um uso particular ou função” e a classificação dos elementos do edifício dada na Tabela 2 na página seguinte, permite a análise que demonstra a correlação predominante de funcionalidade com o subsistema “serviços”, composto basicamente por sistemas prediais que determinam a possibilidade do desenvolvimento da atividade pretendida, seja ela qual for.³

Considerando a hipótese dos sistemas prediais serem suprimidos do edifício, restará tão somente um espaço inerte – que não funciona - portanto, não sendo possível a sua utilização para as atividades propostas, logo, há uma extrema relevância e suma importância do valor agregado por estes sistemas ao funcionamento esperado para o edifício, ainda mais, quando se tratar de um espaço construído para CPD contendo sistemas de MCF-*Mission Critical Facilities*, visando abrigar os equipamentos e suportar as funções de Tecnologia da Informação (TI), essencialmente cruciais aos negócios de uma Instituição Financeira de Classe Mundial.

As mais recentes iniciativas de organizações globais de padronização para ambientes físicos de MCF-*Mission Critical Facilities* estão reconhecendo as necessidades de TI e formulando recomendações, classificações e padronizações, em busca do mais alto desempenho de infra-estrutura básica para os espaços construídos de *Data Centers* (Centros de Processamento de Dados-CPD), sejam eles prédios exclusivos ou ambientes específicos para os ativos de TI inseridos numa parte da edificação, cujos parâmetros encontram-se descritos em padrões de desempenho e aderência (*Performance & Compliance*).

Tabela 2 – Classificação dos Elementos do Edifício*Fonte: ASTM Uniformat II - EL 557-97*

Nível 1 Grupo Principal de Elementos	Nível 2 Grupo de Elementos	Nível 3 Elementos Individuais
A – INFRAESTRUTURA	A10 – Fundações	A1010 – Fundações usuais A1020 – Fundações especiais A1030 - Sapatas
	A20 – Subsolos	A2010 – Escavações A2020 - Paredes
B – ENVOLTÓRIA	B10 – Superestrutura	B1010 – Lajes B1020 – Telhados
	B20 – Vedação Externa	B2010 – Paredes Externas B2020 – Janelas Externas B2030 – Portas Externas
	B30 – Cobertura	B3010 – Telhados B3020 – Lajes Impermeabilizadas
C – ESPAÇOS INTERNOS	C10 – Construções Internas	C1010 – Divisórias C1020 – Portas Internas C1030 - Instalações
	C20 – Escadas	C2010 – Construção das escadas C2020 – Acabamentos das escadas
	C30 – Acabamentos	C3010 – Acabamentos de paredes C3020 – Acabamentos de pisos C3030 – Acabamentos de forros
D – SERVIÇOS	D10 – Transporte	D1010 – Elevadores e monta cargas D1020 – Escadas e esteiras rolantes D1030 – Outros sistemas de transporte
	D20 – Tubulação	D2010 – Instalações de tubulações D2020 – Distribuição predial de água D2030 – Esgoto sanitário D2040 – Águas de chuva D2090 – Outras tubulações
	D30 – HVAC	D3010 – Suprimento de energia D3020 – Sistemas de aquecimento D3030 – Sistemas de refrigeração D3040 – Sistemas de distribuição D3050 – Unidades terminais D3060 – Instrumentação e controle D3070 – Sistemas de teste e balanceamento D3090 – Outros sistemas e equipamentos
	D40 – Proteção ao fogo	D4010 – Sprinklers D4020 – Detectores D4030 – Equipamentos D4090 – Outros sistemas de proteção ao fogo
	D50 – Elétricos	D5010 – Suprimento e distribuição D5020 – Iluminação e ramais D5030 – Comunicação e Segurança D5090 – Outros sistemas elétricos

Os padrões de desempenho e aderência (*Performance & Compliance*), constam de documentos em desenvolvimento, conforme segue :

- Draft ANSI/TIA/EIA-942 (SP-3-0092): *Telecommunications Infrastructure Standard for Data Centers*, em desenvolvimento nos EUA;
- Draft EN 50173-5:200x: *Information Technology – Generic Cabling Systems, Part 5: Data Centers*, em desenvolvimento na Europa;
- Padrão UPTIME INSTITUTE / *Industry Standard Tier Classification Define Site Infrastructure Performance*, definido por este instituto americano que é pioneiro na criação e operação de comunidades do conhecimento em “*Data Center Facilities*” e congrega representantes das maiores organizações em Tecnologia da Informação dos EUA;
- Acervo técnico do “*DATA CENTER USER’S GROUP*” (EUA), contendo os informativos de *benchmarking* compartilhados por diversos profissionais de *Facilities* em Missão Crítica que são representantes das 200 maiores empresas mundiais neste segmento, os quais reúnem-se em congressos internacionais com periodicidade semestral.

A maior prioridade das empresas no contexto atual das redes de comunicações de dados é o seu *data center* (CPD), o qual pode ser desde uma pequena sala no prédio de escritório onde concentram-se os ativos físicos de TI – servidores, roteadores, rack’s de comunicações de dados e outros – até mesmo um prédio exclusivo inteiramente dedicado para abrigar e suportar o “*Hardware & Peopleware*” (equipamentos e pessoas) através de Infra-estrutura de elevada especialização, visando garantir a ininterruptibilidade das mais complexas e críticas funções de TI como nos CPD’s de Instituições Financeiras de Classe Mundial. Durante a última década, a proliferação das redes de microcomputadores em estações de trabalho baseadas em tecnologias de plataformas independentes, tornaram os *data centers* (CPD’s) mais estratégicos do que nunca tanto pelo incremento de produtividade, alavancagem de negócios e aceleração de mudanças, quanto pelo enfoque estratégico dos esforços da Tecnologia da Informação (TI) para proteção, otimização e crescimento da efetividade aos negócios da Organização. O objetivo maior destes esforços de TI é obter uma infra-estrutura ágil que possa incorporar rapidamente os

avanços nas tecnologias de aplicação, armazenagem e processamento de dados, pois, as empresas mudaram as suas definições para *data center* (CPD) de “sala de computadores” para “ativos estratégicos da organização” e a importância de otimização deste ambiente físico vem crescendo de forma acelerada.

Neste cenário, a infra-estrutura física necessária deve ser robusta e versátil o suficiente para suportar uma operação ininterrupta e os padrões globais de classificação estão sendo configurados, endereçando-se as necessidades para uma uniformização de topologias dos recursos prediais, estabelecendo-se os padrões de *Tiers* (Classes) em quatro categorias prediais – Classes I a IV – como descrito abaixo na Tabela 3.

Tabela 3 – Classificação Predial por Recursos do CPD

Fonte: UPTIME INSTITUTE (EUA)

	Classe I	Classe II	Classe III	Classe IV
Número de alimentações	1	1	1 ativo 1 passivo	2 ativos
Redundância de Componente	N	N+1	N+1	2 (N+1) ou S+S
Média de piso elevado do Datacenter	20%	30%	80%	100%
Watts/m²	200-300	400-500	1000-1500	1000-1500
Altura piso elevado	30 cm	45 cm	50-70 cm	50-70 cm
Carga do piso Kg/m²	≤1000	1000	1200	1200-1500
Voltagem utilizada	208	208	13,200/480	13,200/480
Vida útil projetada	3-10	5-15	Ilimitada	Ilimitada
Ano de construção	1965	1970	1990	1994
Tempo de indisponibilidade anual	18.5 h 99.789%	10.3 h 99.883%	3.2 h 99.963%	0.8 h 99.995%

O sistema de padronização das Classes I a IV para CPD's que é utilizado pelo *Uptime Institute* dos EUA, também tem sido verificado nas mais recentes normativas em desenvolvimento pela ANSI e EN para *Data Centers*, sendo importante lembrar que o assunto ainda não se encontra totalmente consolidado, principalmente em âmbito nacional onde ainda não se dispõe de normas específicas, associações de classe ou publicações técnicas que tratem deste assunto com maior profundidade. O procedimento “de praxe” neste mercado costuma ser uma antecipação na adoção das recomendações contidas em normativas internacionais e nos boletins técnicos de associações ou entidades de classe mundiais. Assim, vale lembrar que o sistema de padronização das Classes I a IV para CPD's envolve várias definições sendo importante considerar que um ambiente físico típico de CPD é composto de, no mínimo, 20 (vinte) grandes sistemas prediais nas áreas de mecânica, elétrica, proteção contra fogo, segurança e outras, cada qual com subsistemas e componentes adicionais, sendo que todos estes devem corresponder aos mesmos requisitos de manutenção concorrente ou tolerância à falhas para que o ambiente físico do CPD possa ser classificado desta forma. O resumo de características de cada Classe são descritos na lista a seguir : ²⁶

- ❑ **Classe I (*Tier I*) / Básico** – caminho único de distribuição de força (energia) e de refrigeração (ar-condicionado); sem componentes redundantes; **disponibilidade dos ativos físicos em 99,671%**; constitui-se um *data center* tipo “básico” onde podem ocorrer paralisações dos recursos de ativos físicos tanto em atividades programadas quanto naquelas decorrentes de acidentes (sem possibilidade de planejamento prévio); as instalações contam com sistemas simples (*single bus*) e possuem vários “pontos únicos de falhas”, portanto, esta infra-estrutura requer ao menos uma paralisação geral anual para os trabalhos de manutenções preventivas e corretivas; em situações de emergência podem ser requeridas outras paralisações gerais da infra-estrutura com maior frequência e os erros de operação ou falhas espontâneas de componentes dos sistemas prediais também poderão implicar em interrupções de funcionamento aos equipamentos de TI;

- ❑ **Classe II (Tier II) / Componentes Redundantes** – caminho único de distribuição de força (energia) e de refrigeração (ar-condicionado); componentes redundantes (exemplos: UPS e chillers); **disponibilidade dos ativos físicos em 99,741%**; constitui-se um *data center* tipo “componentes redundantes” onde as possibilidades de paralisações são muito menores que no tipo “básico”, exatamente pela característica de possuir componentes redundantes na infraestrutura básica; as instalações contam com sistemas simples (*single bus*), porém, com módulos de redundância (ex: UPS e chillers) em desenho mínimo de “N+1” (Os módulos necessários + 1 módulo) que facilitam as manutenções em geral; a manutenção de elementos críticos da infra-estrutura básica requer um processo de desligamento dos equipamentos de TI;
- ❑ **Classe III (Tier III) / Manutenção Concorrente** – caminhos múltiplos de distribuição de força (energia) e de refrigeração (ar-condicionado), mas somente um caminho ativo; componentes redundantes; manutenção concorrente; **disponibilidade dos ativos físicos em 99,982%**; constitui-se um *data center* tipo “manutenção concorrente” onde a infra-estrutura básica encontra-se capacitada para realizar as atividades de manutenção sem quaisquer necessidades de interrupção de funcionamento dos equipamentos de TI; as instalações contam com sistemas dualizados (*dual bus*) e componentes redundantes, mas os eventuais erros de operações, acidentes (atividades sem planejamento) e falhas espontâneas de componentes da infra-estrutura básica ainda podem implicar em interrupções de funcionamento dos equipamentos de TI; normalmente neste tipo de *data center* Classe III o projeto permite alcançar a Classe IV, mediante um investimento maior em proteções adicionais preteridas durante a implantação, em face da estratégia de negócios da organização;
- ❑ **Classe IV (Tier IV) / Tolerante à Falhas** – múltiplos caminhos ativos de distribuição de força (energia) e de refrigeração (ar-condicionado); componentes redundantes; sistema tolerante à falhas; **disponibilidade dos ativos físicos em 99,995%**; constitui-se um *data center* tipo “tolerante à falhas” onde a infra-estrutura encontra-se plenamente capacitada para realizar as manutenções sem a

necessidade de interrupções ao funcionamento dos equipamentos de TI, bem como, pode suportar ao menos uma falha não planejada ou evento com possível impacto às cargas críticas, através de, no mínimo dois caminhos ativos de suprimento em infra-estrutura e configuração sistêmica dualizada em desenho “S + S” (1 sistema ativo + 1 sistema ativo); a Classe IV é a categoria de infra-estrutura básica de instalações prediais mais compatível com os conceitos de “Alta Disponibilidade de TI” que envolve as soluções de “CPU *clustering*”, “RAID & DASD” e “Comunicações Redundantes” em busca de melhores índices nos fatores de desempenho, como demonstrado na Tabela 4.

Tabela 4 – Compatibilização dos Recursos de “TI & Facilities”

Fonte : UPTIME INSTITUTE (EUA)

	CONFIABILIDADE	DISPONIBILIDADE	FACILIDADE DE SERVIÇO
Tecnologia da Informação	Clustering RAID DASD Token Ring Automação de console Gerenciamento de Mudança	Partições Lógicas Clustering Espelhamento de Dados Hot Backup Continuidade de Negócios	Hot pluggable Atualizações Hot Micro code Call Home
Infra-Estrutura elétrica	UPS Dual Power Sistema+Sistema	Geradores Dual Power Sistema+Sistema	Geradores Dual Power Sistema+Sistema
Infra-estrutura mecânica	Redundância de componentes Ventiladores e bombas nas UPS	Armazenamento térmico	Tubulação duplicada –dual pipe Armazenamento térmico Planta duplicada
Operação do Datacenter	Automação passiva Gerenciamento de Mudança MAPS/Certificação	Operação 24 horas Compartimentalização Opção de by-pass de falha Peças de reposição no site	Execução de trabalho durante horário comercial Conhecimento e Supervisão local

A conclusão sobre o sistema de categorias de Classes I a IV para *Data Centers*, como descrito acima, aponta para o fato de que, mesmo os tipos “manutenção concorrente” e “tolerante à falhas” que possuem os melhores recursos de infra-estrutura básica e instalações físicas, não podem atender aos requisitos de “5 nines” (99,999%) para disponibilidade de funcionamento dos equipamentos de TI, assim, os esforços do MCFM-*Mission Critical Facilities Management* encontram-se permanentemente focados no desafio do desenvolvimento de novas soluções de projeto e gerenciamento de infra-estrutura básica e instalações físicas de *Data Centers*, visando atender ao contexto de elevadas expectativas de ininterruptibilidade das aplicações de Missão Crítica objeto de Governança em TI.

Finalizando este capítulo, tivemos uma visão panorâmica de Tecnologia da Informação e os ambientes físicos de CPD que abrigam tais soluções, assim, poderemos mais adiante tratar especificamente o planejamento e o Gerenciamento de *Facilities*. Ao oferecer uma pequena amostra de tamanho das questões que envolvem a Tecnologia da Informação, passando por tópicos de elevada complexidade e profundidade, o panorama de TI serviu como um pano de fundo aos reflexos que resultam em múltiplas preocupações na Gestão de Facilidades Prediais de Missão Crítica, onde são exigidos os melhores resultados de confiabilidade, disponibilidade e manutenibilidade de seus recursos, em face da elevada dependência de TI presente em Instituições Financeiras. Da mesma maneira, não pode ser diferente quando se constata que também há uma elevada dependência do Gerenciamento de Facilidades de Missão Crítica para os ativos de TI & Telecom, cuja situação atual premida pelas mais diversas legislações e normativas exige os mais elevados índices de desempenho das instalações físicas que criam as condições oportunas à proposta que consta deste trabalho de um Modelo de Governança em Facilidades Prediais para os Centros de Tecnologia da Informação de Instituições Financeiras Classe Mundial.

Capítulo 3 – PLANEJAMENTO ESTRATÉGICO

Neste capítulo, a visão de planejamento estratégico para Facilidades Prediais de Missão Crítica inclui uma pequena base teórica e alguns elementos práticos que devem contribuir no desenvolvimento de um Modelo de Governança em *Facilities* para a Tecnologia da Informação, o qual abordaremos ao final do presente trabalho.

O planejamento do **Gerenciamento de Facilidades** no setor bancário também pode se valer da expressão “*planejar é determinar os objetivos e os meios eficazes para alcançá-los*” formulada por Ackoff e, nesse processo, uma atividade contínua de análise do futuro é uma exigência lógica e operacional. Do ponto de vista estritamente lógico, os objetivos são vislumbrados e devem se realizar no futuro, cuja análise é, portanto, necessária. Do ponto de vista da eficácia da decisão, é preciso saber “ver antes”, para modificar, aproveitar ou induzir ocasiões a favor da empresa. A experiência mostra que há uma aceleração nas mudanças estruturais (econômicas, políticas, sociais, tecnológicas, etc), causa de rompimento entre os padrões conhecidos no passado e os esperáveis no futuro – os paradigmas do negócio.²⁷

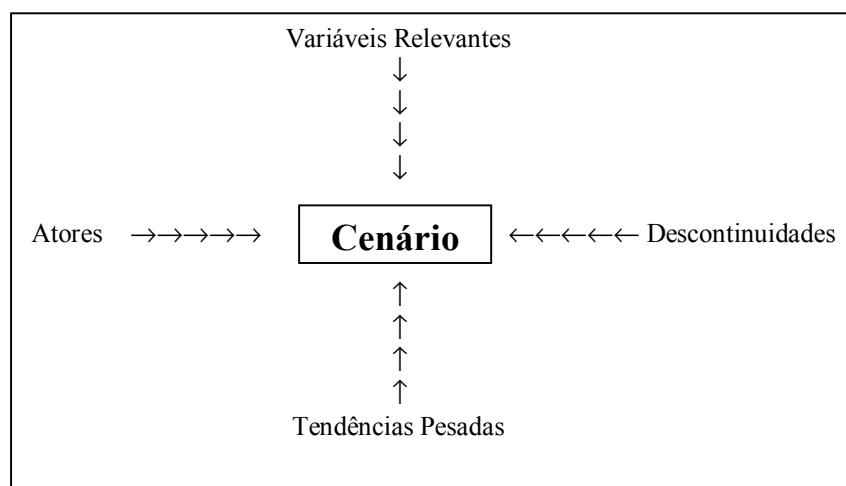
O estudo do futuro implica vencer três grandes dificuldades: i) a incerteza a ser estruturada - explorar configurações futuras e suas variáveis mais relevantes; ii) a complexidade a ser reduzida – definição de um sistema e sua estrutura, correspondendo a um modelo da realidade; iii) a organicidade a ser respeitada – simular situações hipotéticas sobre o comportamento da variáveis e das suas inter-relações. Dessa combinação, resultam os *cenários* definidos como a “*descrição de um futuro possível, com a explicitação dos eventos que levariam a sua concretização*”, ou ainda, como a “*seqüência coerente de eventos futuros hipotéticos*”.²⁸

Os *cenários* apresentam uma ligação imediata e natural com o planejamento estratégico, criando a moldura dentro da qual são estabelecidas as decisões, diretrizes

e prioridades para a ação. A definição das variáveis relevantes dos cenários é feita a partir das variáveis relevantes do “negócio” ou “âmbito de atuação da organização” e os demais componentes principais são os atores, as discontinuidades e as tendências pesadas, conforme mostrado abaixo na Figura 17.

Figura 17 – Principais componentes de um cenário

Fonte : AUTOR



Assim, discorrer sobre planejamento não é tarefa fácil, em face da profusão de abordagens e mesmo de métodos, os quais trazem certa confusão em suas aplicações e levam ao senso comum de que planejar não conduz a resultados. Paradoxalmente, os estudiosos e gerentes têm hoje, a sua disposição, uma profícua literatura dirigida à atividade empresarial referente ao termo planejamento e isto, em parte, foi devido ao intensivo processo de competitividade que então se desencadeou em nível internacional, levando à busca incessante por saídas estratégicas. Deve-se, ainda, levar em consideração que, atrás do vocábulo planejamento, pode-se aduzir de forma ampla, uma infinidade de outros temas afins, tais como prospectiva, estratégia, plano, projeto, objetivos, visão estratégica e cenários, dentre outros. Por outro lado, há ainda de ser lembrada a questão da temporalidade do planejamento: curto, médio ou longo prazos.

O planejamento enquanto processo de mudança de situações incômodas, deficientes e carentes, não pode prescindir de uma adjetivação, precisamente, de seu caráter

estratégico e isto quer dizer que nenhum *ator* pode implementar planos sem levar em consideração as circunstâncias (adversas ou não) em que serão executados, pois, o jogo dos planos é uma arena em que se digladiam atores convergentes (que aderem ao plano) e atores divergentes (que rechaçam o plano). A partir dos anos de 1980 as empresas do setor privado passaram a formular os seus planejamentos estratégicos corporativos e este modelo contempla a análise do ambiente em que se insere a empresa, identificando seus pontos fortes e fracos (internos) e as ameaças e oportunidades (externas) para conhecer a aderência e a oposição a seus objetivos, neste caso, a empresa está preocupada com seus concorrentes e com a adesão (aquisição/compra) pelo consumidor, a seus produtos e/ou serviços.²⁹

Assim entendido, o planejamento estratégico do **Gerenciamento de Facilidades** de Missão Crítica para TI representa a identificação da infra-estrutura e instalações necessárias para garantir a oferta de segurança operacional aos bens e serviços, de maneira a suportar a evolução prevista em Tecnologia da Informação de apoio aos negócios da Organização.

3.1 Resumo de Propostas

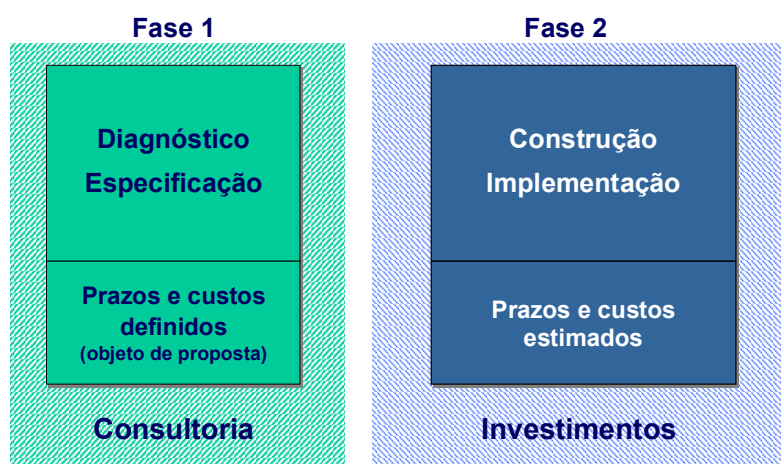
As questões mais abrangentes do planejamento estratégico de Gerenciamento de Facilidades de Missão Crítica para TI devem ser tratadas e abordadas com a visão de um diagnóstico geral, alinhado com as necessidades de todas as áreas de Tecnologia da Informação da Instituição Financeira de Classe Mundial, com a finalidade de identificar problemas, necessidades e alternativas para solução, como resultado de um trabalho a ser realizado, onde deve ser apresentado um parecer técnico da *situação atual*, os requisitos da *situação desejada* e a definição de uma estratégia para *atendê-los*. A partir de entrevistas individuais com os diretores das áreas de TI devem ser identificadas as *frentes de trabalhos* e seus respectivos *projetos*, com o

objetivo final de imprimir excelência na prestação dos serviços de TI aos seus clientes internos e externos.

A visão total de cada *projeto* deve considerar, no mínimo, duas fases principais conforme demonstrado abaixo na Figura 18, sendo: a) Fase 1 – Consultoria (diagnóstico e especificação, contendo os prazos e custos definidos no resumo das propostas); b) Fase 2 – Investimentos (construção e implementação, com indicação dos prazos e custos estimados).

Figura 18 – Visão Total do *Projeto*

Fonte : CPM



As propostas para o planejamento estratégico do **Gerenciamento de Facilidades** devem considerar, no mínimo, 05 (cinco) pontos básicos, conforme segue: ³

- ♦ **Gerenciamento de Valores** – além de buscar a efetividade dos custos deve-se também observar outros objetivos como a estratégia dos negócios e a imagem da organização perante o mercado. O componente financeiro é apenas um dos componentes da análise, cujo valor de um serviço deve ser associado também à funcionalidade, desempenho e qualidade;

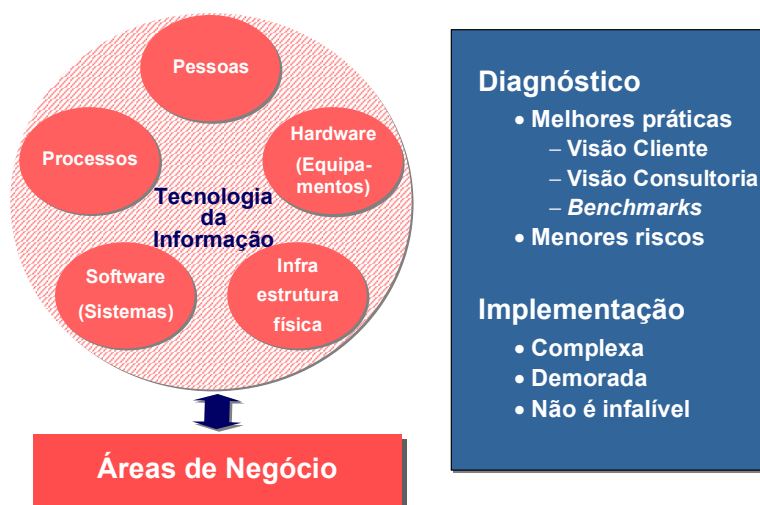
- ♦ **Gerenciamento Ambiental (Externo/Interno)** - o quesito macro-ambiental externo está fortemente relacionado com o consumo de energia, o uso racional da água (este bem finito e escasso) e o tratamento dos resíduos produzidos pelo edifício, sejam nas etapas de construção ou operação. Internamente ao edifício, a gestão ambiental está principalmente relacionada com a qualidade do ar interno (IAQ-*Indoor Air Quality*) , ou seja, a saúde dos usuários do edifício com reflexos nas atividades desenvolvidas por produtividade ou absenteísmo;
- ♦ **Gerenciamento da Qualidade** – deve objetivar a satisfação das necessidades dos usuários com todos os processos e atividades relacionados aos serviços providos, cujos princípios podem ser alcançados através da implementação de Círculos de Controle da Qualidade;
- ♦ **Gerenciamento de Riscos** – identificar possíveis ameaças à implantação daquilo que foi planejado em nível estratégico e estabelecer procedimentos que procurem garantir que limites toleráveis não sejam ultrapassados, o que pode ser conseguido através de : a) manuais de operação precisos, inteligíveis e disponíveis; b) treinamento constante do pessoal envolvido com operação e manutenção; c) existência de dispositivos e sistemas de alarme; d) confiabilidade operacional elevada para os componentes e sistemas críticos – redundância, dualidade, flexibilidade e recursos com folga;
- ♦ **Gerenciamento de Mudanças** – condução das pessoas através dos processos de mudanças, envolvendo e fazendo com que participem da condução destes através de trabalhos em equipe, mantendo-as esclarecidas sobre os objetivos finais e informadas permanentemente sobre o andamento dos trabalhos, visando cooperarem para o sucesso do empreendimento.

O planejamento estratégico do Gerenciamento de Facilidades de Missão Crítica deve estar alinhado ao Diagnóstico de TI envolvendo as cinco dimensões principais, conforme descrito a seguir na Figura 19. Assim, as análises podem ser confrontadas com as necessidades das áreas de negócios da Organização, avaliando-se a composição do diagnóstico de acordo com as melhores práticas na visão do Banco,

na visão da Consultoria e nos *benchmarks* de mercado, buscando-se os menores riscos ao caso concreto sob avaliações e considerando-se, desde logo, que a fase de implementação pode ser complexa, demorada e não pode ser considerada infalível.

Figura 19 – Dimensões do Diagnóstico de TI

Fonte : CPM



O Diagnóstico de TI contido na Fase de Consultoria do *Projeto*, onde encontram-se as especificações com prazos e custos definidos, deve considerar algumas premissas básicas ao resumo das propostas, conforme segue :

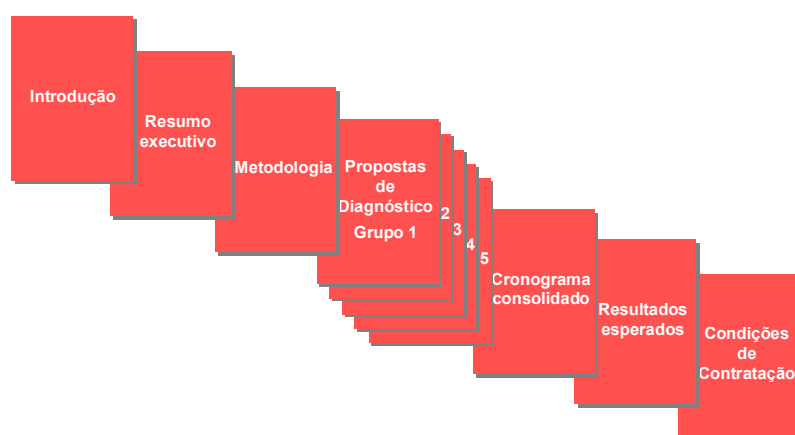
- ✓ Todos os diagnósticos devem avaliar as iniciativas da Instituição Financeira de Classe Mundial (cliente) e os *projetos* já em andamento em cada uma das frentes;
- ✓ A Consultoria deve atuar de forma transparente e crítica, com independência de opinião, buscando recomendar a melhor alternativa para o seu cliente;
- ✓ Os resultados de cada *projeto* devem ser entregues tão logo finalizados, gerando benefícios imediatos para o cliente;
- ✓ O cliente deve destacar os recursos necessários para atuarem como facilitadores nas etapas de levantamentos e diagnósticos da Consultoria;

- ✓ Os trabalhos da Consultoria devem ser executados preferencialmente com recursos próprios, exceto quando capacitações especiais forem necessárias, neste caso, admitindo-se a utilização de empresas parceiras, mediante prévia consulta ao cliente;
- ✓ Após o *projeto* de diagnóstico, a Consultoria deve atuar como implementadora e/ou gerenciadora do *projeto* final;

O conteúdo das propostas deve abranger, em resumo, os aspectos definidos conforme demonstrativo abaixo que consta da Figura 20.

Figura 20 – Conteúdo das Propostas

Fonte : CPM



O sumário executivo das propostas, em última análise, deve considerar as observações básicas e preliminares do seguimento de Tecnologia da informação (TI), tais como: i) TI precisa de aprimoramento contínuo das ferramentas de gestão, compatíveis com as mais recentes necessidades (metas e indicadores para os níveis de serviços prestados às áreas de negócios da organização; controle integral dos processos internos de TI); ii) necessidade de valorização crescente do papel da Tecnologia do Negócio (TN) – aumentar o escopo de atuação e aumentar a

responsabilidade/autoridade no processo de atendimento às demandas - como parte integrante da área de Tecnologia da Informação (TI); iii) uma maior sintonia de objetivos entre TI e Áreas de Negócios da Organização pode melhorar a qualidade dos serviços prestados pela empresa; iv) a constatação de dificuldade intrínseca de TI em justificar e aprovar investimentos em melhorias de seus recursos.

Assim, a área responsável por sistemas de Facilidades Prediais de Missão Crítica em Instituição Financeira de Classe Mundial, encontra um momento favorável ao lançamento de um **Plano Básico de Reestruturação**, visando a atualização do modelo existente e alinhamento às mais recentes boas práticas do mercado, desta forma, sendo capaz de estabelecer um contexto facilitador ao crescimento e desenvolvimento pleno do potencial que tem, como elemento fundamental e crucial no suporte das funções estratégicas de Tecnologia da Informação (TI), responsável por alavancar a vantagem competitiva e negócios da Organização.

3.2 Metodologia-Etapas

A metodologia de planejamento estratégico aplicada no **Gerenciamento de Facilidades** de Missão Crítica deve ser concebida como parte integrante da área de TI, mediante um pleno alinhamento que represente a identificação da infra-estrutura e instalações necessárias para garantir a oferta de segurança operacional aos bens e serviços, de maneira a suportar a evolução prevista em Tecnologia da Informação de apoio aos negócios da Organização, cujo o conjunto de análises pode ser dividido em 05 etapas básicas : i) situação atual; ii) situação desejada; iii) diagnóstico; iv) plano de ação; v) justificativas. A análise da **situação atual** define onde a área de TI encontra-se hoje e representa a identificação dos processos, necessidades e problemas em cada uma das frentes de trabalho. O desenho da **situação desejada** define onde a área de TI deseja estar no futuro e representa a definição da situação

desejada, com base nas referências aceitas pela Instituição Financeira de Classe Mundial sob enfoque e nos *benchmarks* representativos das melhores práticas. O estabelecimento de um **diagnóstico** define quais são os desafios e as oportunidades do processo e representa a identificação dos *gaps*, formulação propriamente dita do diagnóstico, qualificação das oportunidades de melhorias e recomendações técnicas. O **plano de ação** define como a área de TI poderá chegar lá e representa a elaboração efetiva do plano com atividades, recursos e prazos que permitam migrar da situação atual para a situação desejada. As **justificativas** definem o por que de se executar o projeto e representa a formulação de argumentação positiva com base nos custos, investimentos estimados e benefícios esperados.

Portanto, assim considerada, a metodologia proposta estabelece uma matriz de cinco etapas prioritárias onde o conjunto de atividades principais podem ser divididos conforme segue : ³⁰

- ◆ **Etapla 1 - Situação Atual** : são efetuadas reuniões, visitas, entrevistas e o relatório de situação, contendo os problemas identificados, possíveis causas, necessidades, alternativas de atendimento, medições de desempenho (níveis de serviços), outros requisitos e restrições;
- ◆ **Etapla 2 – Situação Desejada** : são efetuados os levantamentos de visão dos gestores, visão de TI e visão de mercado para produzir o relatório de referências e *benchmarks*, contendo a lista de referências avaliadas, o descritivo de visitas e entrevistas realizadas, as premissas adotadas, bem como, a descrição da situação desejada e seus requisitos;
- ◆ **Etapla 3 – Diagnóstico** : são identificadas as oportunidades, os *gaps*, as prioridades, os objetivos e metas, bem como as recomendações de melhorias que levarão a área de TI à situação desejada;
- ◆ **Etapla 4 – Plano de Ação** : são descritas as atividades e dependências, as prioridades, as responsabilidades, os prazos e os fatores críticos de sucesso que se deve seguir para migrar da situação atual para a situação desejada;
- ◆ **Etapla 5 – Justificativas** : com base no plano de ação aprovado, nesta etapa devem ser apresentados os benefícios e as justificativas técnicas e financeiras.

O momento de estudo da metodologia-etapas também pode ser o mais apropriado ao desenho de organização dos projetos, considerando cada frente de trabalho definida na Fase de Consultoria e os recursos necessários para gestão (tática/estratégica) e equipes técnicas operacionais, tanto na coordenação interna quanto de terceiros envolvidos, de modo a estabelecer o organograma de atuação dos diversos postos de trabalho envolvidos na hierarquia dos projetos.

3.3 Resultados Esperados

Os resultados esperados no processo de planejamento estratégico do **Gerenciamento de Facilidades** de Missão Crítica encontra-se totalmente focado nas perspectivas e dimensões dos resultados associados à Tecnologia da Informação, sendo considerada a questão de temporalidade do planejamento: curto, médio ou longo prazos. Desta forma, o maior objetivo constitui-se na busca por redução de riscos e melhoria de resultados, satisfação dos usuários e qualidade da gestão dos recursos de TI, representada por ações integradas em cinco dimensões com vários projetos distintos tantos quantos sejam necessários.

Assim estruturado o trabalho, os resultados esperados em escalas complementares dos níveis de desempenho e de gestão, são os seguintes :

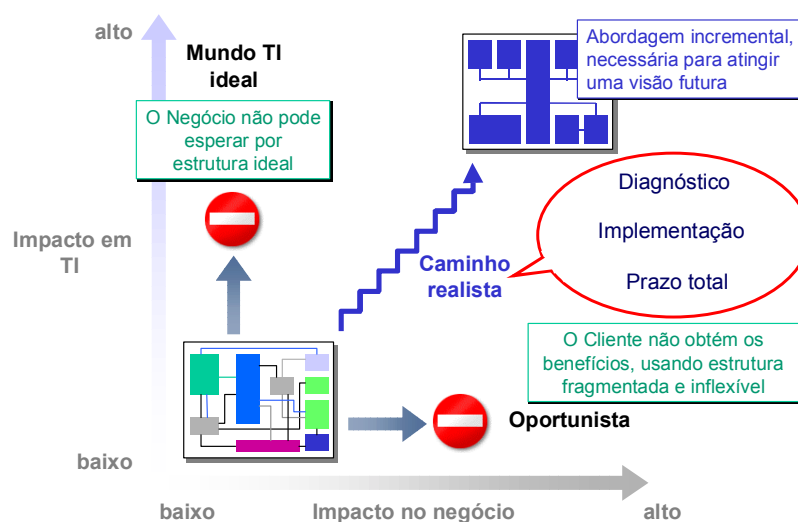
- ❖ **Curto Prazo** – melhor nível de serviços; gerenciamento de fatores que geram incidentes; resultados no decorrer dos trabalhos;
- ❖ **Médio/Longo Prazos** – maior satisfação de usuários e clientes; maior rapidez de resposta ao mercado; redução de retrabalho e ineficiências; menores riscos operacionais; redução de custos e despesas;

Em abordagem do processo de migração da **situação atual** para a **situação desejada** são relevantes as análises de impactos de TI&Negócios (baixo/alto), confrontando-se

as necessidades do mundo ideal de TI e o aspecto oportunista de Negócios, com seus fatores de influências mútuas, visando-se definir o caminho realista de implementação do **diagnóstico** efetuado, contemplando todos os fatores contidos no **plano de ação e justificativas** ao proposto, assim sendo, possibilitando estabelecer uma abordagem incremental necessária para se atingir os **resultados esperados** para a visão de futuro do planejamento, conforme demonstrado abaixo na Figura 21.

Figura 21 – Abordagem de Migração nas Etapas do Planejamento

Fonte : CPM



Neste estudo de planejamento estratégico foram abordados tópicos que tratam da infra-estrutura necessária para o desenvolvimento das funções do **Gerenciamento de Facilidades de Missão Crítica para TI**, com a definição das linhas gerais que norteiam a sua prática, tratando de questões abrangentes e de longo prazo no processo desenvolvido pelas áreas de Tecnologia da Informação, objetivando alinhar os propósitos da **Gestão de Facilities** com os objetivos estratégicos de TI no suporte aos negócios da Organização, resultando no entendimento dos procedimentos que possibilitam saber o que deve ser feito e por que e oferecendo todas as bases para o sucesso do planejamento estratégico, o qual dependerá da correta implantação em nível operacional daquilo que foi idealizado, ou seja, a evolução deste processo para

a definição do planejamento tático que, efetivamente, permitirá a implantação da Gestão Completa de Infra-estrutura e Instalações descrita na proposta de um modelo expresso pela idéia do **“Gerenciamento de Facilidades como Alavanca de Negócios no Setor Bancário”**, o qual denominamos como Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras.

Encerrando este capítulo, vimos os patamares adequados de organização das idéias em planejamento estratégico para Facilidades Prediais de Missão Crítica, o qual vai possibilitar o desenvolvimento da proposta de um modelo de Governança em *Facilities* ao final do presente trabalho.

Capítulo 4 – ESPECIFICAÇÕES DE PADRÕES PREDIAIS

Neste capítulo, o alvo das considerações é a necessidade de especificações de padrões prediais confiáveis, definidos e balanceados que possam garantir a segurança operacional do CPD, assim, serão tratadas as questões dos diversos sistemas prediais presentes no ambiente físico de Missão Crítica em Tecnologia da Informação de Instituições Financeiras de Classe Mundial.

Os espaços construídos destinados a abrigar aplicações de Tecnologia da Informação (TI) apresentam necessidades especiais em face dos requisitos de segurança operacional, visando o máximo resultado de desempenho na tríade essencial de premissas fundamentais – disponibilidade, confiabilidade e manutenibilidade – requeridas na visão de uma Gestão Completa de Infra-estrutura e Instalações para as Facilidades de Missão Crítica em TI. O projeto deste tipo de edificação produtiva deve ser concebido com base nos conceitos de ambiente seguro, aplicados às condições intrínsecas do local escolhido, especialmente preparado para ser plenamente adaptável às funções da atividade-fim de TI no suporte aos negócios da Organização, alinhando-se ao conceito do Gartner Group que consta da afirmação a seguir :

“Do not build to last – Build to change” (agosto/2003)

(não construa para ficar, mas para mudar)

A flexibilidade constitui-se qualidade fundamental de projeto que facilita as mudanças, portanto, reduz os riscos inerentes em alterações dos ambientes físicos e sua infra-estrutura e instalações, assim, o espaço construído para ambientes de Missão Crítica em TI têm sido alvo de esforços nas especificações de padrões prediais, tanto no sentido de classificar o desempenho físico da edificação como um todo, quanto de seus sistemas prediais ou até mesmo de subsistemas que compõe as soluções de *Facilities* para as áreas de Tecnologia da Informação.

As diversas frentes de trabalho em andamento para normalização das características de confiabilidade e mensuração de resultados do desempenho físico em espaços construídos que abrigam e suportam os equipamentos e funções de TI, tanto em âmbito internacional com seus avanços mais evidentes quanto no âmbito nacional onde também se verificam esforços concentrados, percebidos em atitudes pró-ativas de novas associações, institutos, meios acadêmicos e agências reguladoras, ora iniciam um processo de consolidação de uma nova faixa funcional dentro do universo empresarial brasileiro, o qual passa a ser conhecido como “*Facilities*” sendo responsável por uma complexa infra-estrutura de suporte aos negócios da organização e seu sistema produtivo - a sua cultura, estratégias, informações, propriedades, valores intelectuais, todos os insumos diretamente utilizados em seus portfólios e, principalmente, seus valores humanos com as suas respectivas necessidades. Assim entendido, o foco fundamental do *Facilities* passa a ser o de determinar “como” a empresa pode ser adequadamente estruturada para suportar o seu complexo produtivo de maneira eficiente e eficaz, utilizando-se do perfil multidisciplinar exigido por este segmento, contando com capacidades técnicas e administrativas (engenharia, arquitetura, administração, direito, TI, governança, dentre outros) e sendo temperados por elementos especiais de psicologia, diplomacia, simpatia e extrema capacidade de inter-relação pessoal, isso tudo, visando alcançar um modelo de Gestão Completa de Infra-estrutura e Instalações objeto de elevada efetividade ao ser projetado, administrado, mantido e constantemente atualizado, ao tornar-se um forte diferencial estratégico da empresa perante o mercado, devido aos altos custos operacionais que representa e o elevado valor agregado no controle de riscos operacionais, de responsabilidade sócio-ambiental, de reputação e imagem da Organização.³¹

Mais de 60 organizações de classe mundial no seguimento de *Facilities* de Missão Crítica para Tecnologia da Informação e Telecomunicações (incluindo-se fabricantes, consultores, usuários e outras organizações) encontram-se contribuindo com suas “*expertises*” para o desenvolvimento de especificações de padrões prediais visando prover recomendações e “*guidelines*” (guias) para o projeto (desenho) e instalações de *data centers* (CPD’s) ou salas de computadores. O propósito de se

criar um padrão de recomendações tem por objetivo o de capacitar o planejamento prévio dos requisitos do *data center* no processo de desenvolvimento do espaço construído, contribuindo nas considerações de arquitetura, provendo informações relevantes e promovendo um contexto colaborativo no curso dos esforços multidisciplinares de projeto e fases da construção. O planejamento adequado durante a construção ou reformas da edificação pode produzir reduções significativas de custos e das interrupções de funcionamento do que depois que as instalações encontram-se em operação normal. Preliminarmente, os *data centers* apresentam duas categorias básicas de acordo com o tipo de uso ou função, a primeira quando em domínio privado onde podem ser classificados como EDC-*Enterprise Data Center* e a segunda quando em domínio público onde podem ser classificados como IDC-*Internet Data Center*, CDC-*Colocation Data Center* ou SPDC-*Service Provider Data Center*. Nestes ambientes de Tecnologia da Informação e Telecomunicações, encontrados em corporações privadas, instituições ou agências governamentais, as **Facilidades de Missão Crítica (FMC)** incluem soluções visando oferecer energia segura, controles ambientais, proteção contra fogo, redundância de sistemas e segurança física aos ativos da Organização.³²

De acordo com as metodologias aplicadas em diversos estudos de padronizações em desenvolvimento, as especificações encontram-se divididas em duas categorias de critérios a serem aplicados nestas recomendações – mandatórios e recomendáveis. Os critérios mandatórios passam a ser designados pela palavra “**deve**” e visam estabelecer os requisitos mínimos aceitáveis, segundo a visão do presente trabalho, por outro lado, os critérios recomendáveis ou desejáveis passam a ser designados pela palavra “**pode**” e visam incrementar o desempenho dos sistemas prediais sob enfoque. As especificações e recomendações aplicadas neste contexto tem por objetivo oferecer um conjunto de requerimentos mínimos aplicáveis numa visão de Gestão Completa de Infra-estrutura e Instalações em Prédios de Missão Crítica para TI, representando os requerimentos de uma série de apontamentos encontrados em normativas de agências reguladoras, associações, institutos e entidades de classe de âmbitos nacional e internacional, conforme referências bibliográficas citadas ao final do presente trabalho.

4.1 Diretrizes Construtivas

Ao se analisar as diretrizes construtivas para a definição da edificação destinada para abrigar e suportar equipamentos e funções de TI, antes de tudo, se faz de maior relevância e importância considerar alguns conceitos para a escolha de localização do Site de Missão Crítica - *Data Center* (CPD-Centro de Processamento de Dados), NOC, SOC, CC e *Energy Plant*. O local é fator fundamental da segurança, entretanto, não existe local perfeito, totalmente livre de qualquer ameaça de inundação, alagamento, poluição acidental, vizinhança combustível, trânsito com cargas perigosas, tráfego aéreo, terroristas, comoção civil, piquetes e outros. O balizador principal das direções a serem tomadas no objetivo de se estabelecer as especificações de padrões prediais visando garantir a máxima segurança operacional nos Ambientes de Missão Crítica em Instituições Financeiras de Classe Mundial, resulta dos planejamentos estratégico e tático do Gerenciamento de Facilidades, contendo as análises de riscos efetuadas em Projeto de Plano de Contingência, uma vez que eventual perda de informações e seus custos associados orientam completamente o desenvolvimento, a execução ou adequação do espaço construído do Prédio de Missão Crítica, uma vez que a destruição física dos sistemas é um evento irreversível ou até mesmo a interrupção temporária de acesso aos dados pode ser prejudicial, pois mesmo que os dados estejam bem guardados não poderão ser utilizados pelos usuários e clientes da Organização.

A definição de conceitos preliminares para a localização do Prédio de Missão Crítica de TI deve considerar algumas premissas básicas prévias ao desenvolvimento de um catálogo detalhado de recomendações, conforme descrição a seguir :²¹

- i. A exposição do local em relação às ameaças reais precisa ser compensada por medidas especiais na construção e na infra-estrutura, através de instalação de sistemas de segurança e ainda, por medidas organizacionais;

- ii.O campo em volta do prédio deve oferecer cerca ou outro tipo de barreiras contra acidentes e lançamento intencional de veículos;
- iii.O subsolo deve ser drenado por caimento evitando-se a utilização de sistema de bombeamento de recalque;
- iv.A localização do prédio deve ser discreta sem chamar a atenção de transeuntes ou vizinhanças;
- v.O local deve possuir acessos garantidos em caso de greves com piquetes, inundação ou outros eventos previsíveis;

Os conceitos de construção e disposição a serem aplicados nas diretrizes para os espaços construídos que abrigam *Data Center* (CPD) devem prever o isolamento dos ambientes de maior criticidade (salas de computadores) em relação às áreas e atividades alheias aos mesmos, bem como, deve buscar a contenção dos riscos de origem interna e externa ao prédio. Assim, a disposição de lay-out deve permitir *setorização* (separação de áreas), atendendo as necessidades específicas de climatização (HVAC), do controle de acessos e da segurança contra incêndios, além dos materiais utilizados na construção, nas instalações e no mobiliário que também devem ser alvo de escolha criteriosa visando limitar a carga combustível. Desta forma, os conceitos construtivos deve considerar as premissas básicas descritas a seguir :²¹

- i.O prédio deve possuir uma proteção perimetral robusta contra a penetração de pessoas, no mínimo equivalente a uma parede de alvenaria de meio tijolo maciço (EN 1627), preferencialmente sem janelas, sendo o padrão corta-fogo correspondente ao fator F-120 (DIN 4102 ou ASTM 119);
- ii.A cobertura deve possuir proteção redundante contra águas pluviais, inclusive tranbordo seguro;
- iii.Os ambientes operacionais devem estar segregados entre si e com relação às áreas comuns, sendo que, o ambiente mais crítico (sala de computadores) deve operar exclusivamente dentro de compartimento com proteção certificada;
- iv.Os ambientes resfriados precisam de isolamento térmico e barreira de difusão;

- v.O prédio precisa oferecer caminhos amplos e seguros para acomodar cabeamento horizontal e vertical;
- vi.O prédio precisa oferecer altura piso-teto (pé-direito) e capacidade de carga compatível com o padrão adotado (sempre maior que 3,5 metros e maior que 500 kg/m^2);

O detalhamento destas premissas básicas deve agrupar todos os levantamentos efetuados em análises da **situação atual** do estudo de caso, visando estabelecer as recomendações específicas necessárias para que se obtenha a compleição das exigências normativas e dos objetivos estratégicos do **projeto** baseado no que há de melhor em tecnologia e em conceitos para atender as Instituições Financeiras de Classe Mundial.

4.2 Fornecimento e Distribuição de Energia

Os conceitos de infra-estrutura elétrica abrangem vários fatores, tais como: a disponibilidade de energia (com e sem interrupção), a qualidade de energia (aterramento, supressão de surtos, filtragem, harmônicos, dentre outros), a adaptabilidade (modularidade e estrutura de cabeamentos), a proteção física e elétrica dos sistemas de energia, o monitoramento, a detecção, a manutenção, enfim, o gerenciamento completo da matriz energética do Prédio de Missão Crítica.

Neste tópico devem ser examinados todos os requerimentos elétricos, análises de dimensionamento de carga e recomendações para adotar uma proposta de sistema elétrico para um CPD. Como premissa básica, um sistema de fornecimento e distribuição de energia para CPD deve operar 24 horas/365 dias com a máxima

confiabilidade no tocante às quedas de energia para cargas de missão crítica, bem como, de elevada flexibilidade para manutenções preventivas e corretivas, sem a necessidade de interrupções de funcionamento no sistema e, conseqüentemente, na carga de missão crítica.

O fornecimento de energia em média tensão deve se dar em no mínimo duas linhas em classe 15kV ou 35kV - 60Hz, a serem reduzidas para o suprimento em baixa tensão através de subestação transformadora em média tensão, sendo aconselhável que estas duas linhas derivem de subestações primárias independentes, visando uma maior confiabilidade do sistema, com as linhas em percursos independentes e separados entre si por mais de 20 metros. O CPD deve ter dois tipos de distribuição de energia que podem ser assim classificados – Energia Essencial e Energia Crítica.

A Energia Essencial visa alimentar as cargas essenciais que poderão sofrer quedas momentâneas de energia (0 a 30 segundos), até que o(s) gerador(es) de emergência assumam(m) toda a carga do CPD. Os sistemas UPS-*Uninterruptible Power System* (no-break), retificadores, ar-condicionado, iluminação e tomadas de uso geral são alguns exemplos de cargas essenciais. A Energia Crítica visa alimentar as cargas críticas que, em nenhuma hipótese, poderão sofrer uma queda de energia, ou seja, aquelas que tem por objetivo os requisitos de disponibilidade máxima em busca do índice 100% de ininterruptibilidade, sendo que tais cargas devem ser alimentadas por sistemas UPS's, como por exemplo, os equipamentos de TI tais como os Mainframes, Servidores, Salas-Cofre, Teleprocessamento, Segurança, dentre outros.

A provisão de componentes redundantes em cada segmento do sistema elétrico visa torná-lo um sistema de maior confiabilidade, apropriado para ambientes de missão crítica, sendo a configuração mínima de redundância denominada de N+1 (obs: o "N" corresponde ao número de unidades necessárias e +1 unidade de reserva), porém, em algumas partes do sistema onde a confiabilidade deve ser ainda maior, como por exemplo nos UPS's, demonstra-se oportuna a utilização de sistema 2(N+1) ou 2N ou S+S (obs: quando duas vezes o número de unidades necessárias, ou seja, dois sistemas completos). Quando se tem apenas uma fonte de energia comercial, se

faz recomendada a instalação de geradores de emergência em configurações $2N$ ou $N+2$ ou $N+1$. Um sistema de fonte de energia ininterrupta UPS, o qual visa manter a energia segura para a carga crítica durante períodos de queda de energia da concessionária, no intervalo de tempo enquanto o sistema de geração de emergência *stand-by* se habilita para assumir a carga, deve ser instalado preferencialmente na configuração $2(N+1)$ ou $2N (S+S)$, contando com um sistema de refrigeração exclusivo que deve suportar o sistema UPS e a carga crítica, o qual também deve ter uma configuração mínima de $N+1$.²⁶

O modelo ou configuração de redundância, além de aumentar a confiabilidade do CPD em termos falha de energia e de ar condicionado, facilita todo o processo de manutenção, cujos procedimentos podem ser executados sem que a carga crítica seja afetada, sendo isto válido para os sistemas de geração de emergência, subestações de energia, quadros de distribuição elétrica, barramento elétrico, PDU's, fontes de corrente contínua (retificadores ou UPS DC) e sistemas de ar condicionado.

Atualmente o Estado da Arte em projetos elétricos de missão crítica em todo o mundo, tem se utilizado de sistemas denominados de *dual-bus* ou *three-bus* (duas ou três linhas independentes de alimentação e distribuição de energia) como padrão geral do sistema elétrico, cujo contexto de minuciosas discussões entre as vantagens e desvantagens de cada sistema pode conduzir à opção pela recomendação de uso do melhor sistema elétrico em cada aplicação para CPD. O sistema elétrico deve ser projetado de acordo com as normas ABNT-Associação Brasileira de Normas Técnicas e, quando necessário, obedecendo também a critérios internacionais de normalização, além de leis federais, estaduais, municipais e normas internas de cada cliente. A título de ilustração, constam das Figuras 22, 23 e 24 os desenhos básicos e comparações de vantagens e desvantagens, dos sistemas elétricos *Single-Bus*, *Dual-Bus* e *Three-Bus* que podem ser recomendados para o uso em CPD's, de acordo com o níveis de confiabilidade, disponibilidade e classificação geral que se pretende atingir para o ambiente físico de TI.²⁶

Figura 22 – Exemplo de Sistema Elétrico Single-Bus

Fonte : SISTENGE

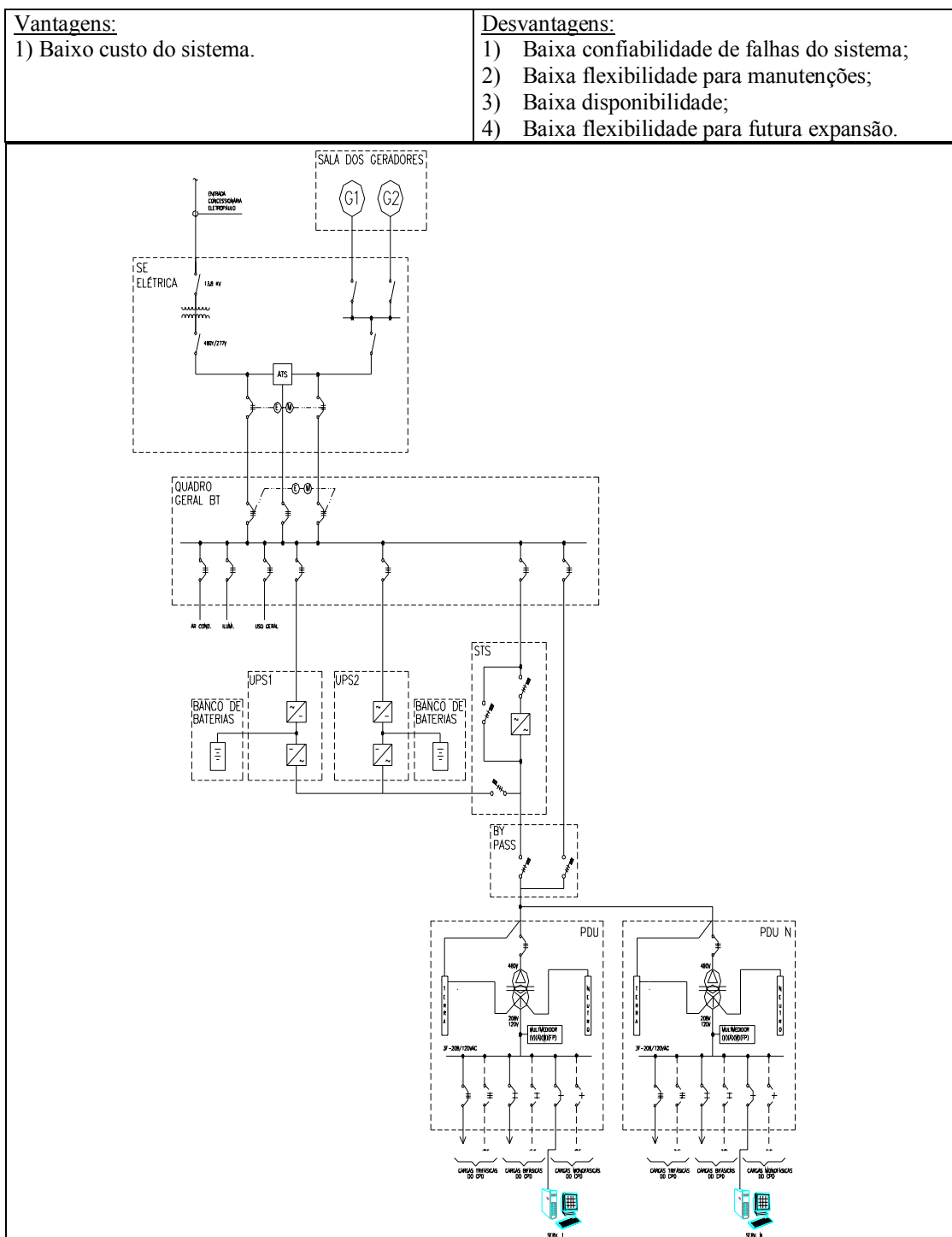
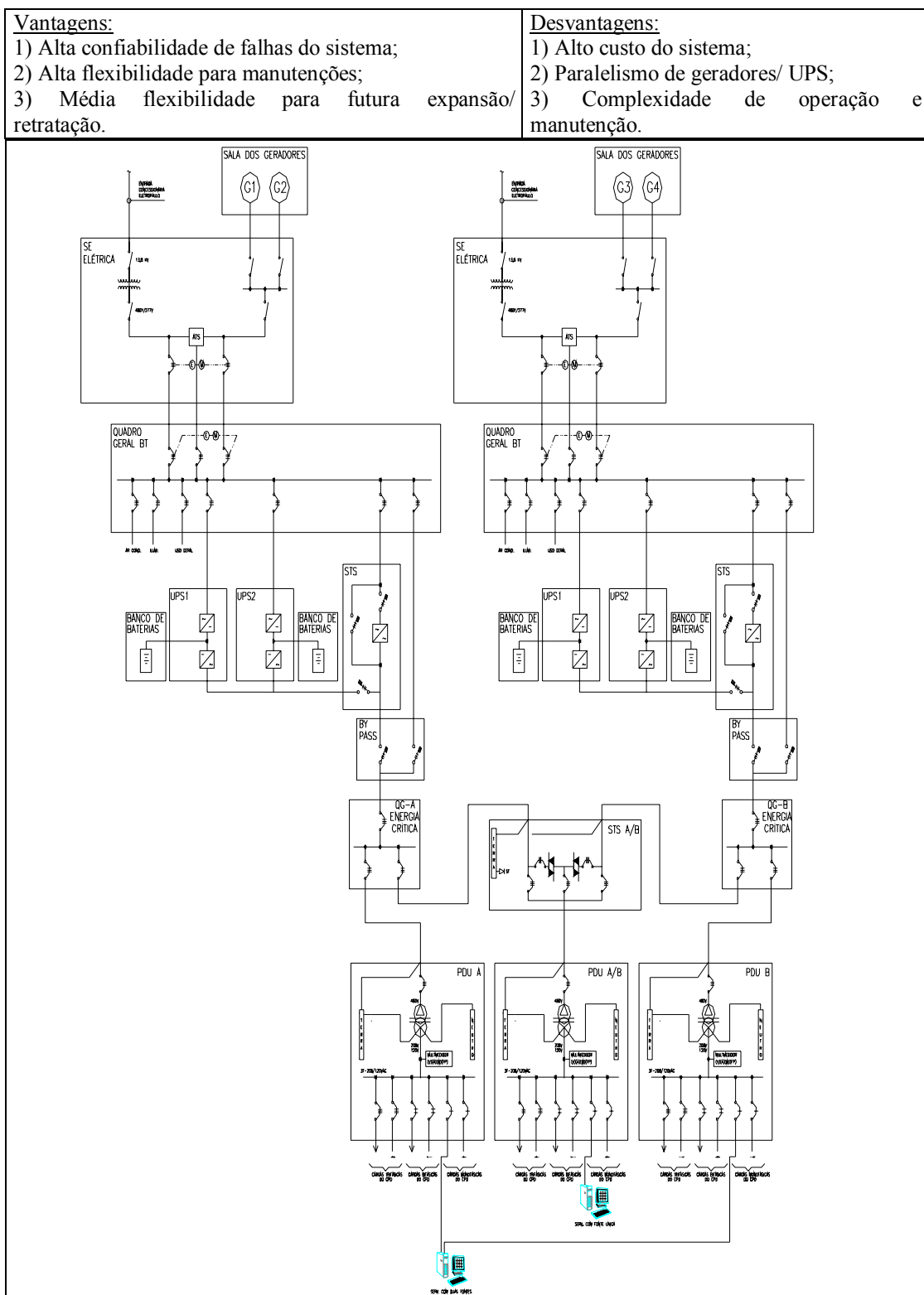


Figura 23 – Exemplo de Sistema Elétrico Dual-Bus*Fonte : SISTENGE*

Com base em levantamentos de consumo elétrico do cliente e baseando-se também nos padrões mundiais utilizados em construções de CPD's, com indicadores de kVA/m² e TR/m², considerando-se as premissas de anteprojeto de arquitetura que possa indicar as características construtivas do Prédio CPD sob análise, há possibilidade de serem sugeridos os estudos preliminares com o dimensionamento básico de todo o sistema elétrico visando estabelecer o consumo total de potência aparente do CPD que pode chegar à patamares em torno de 6MVA no sistema elétrico primário no Site Principal de Instituição Financeira de Classe Mundial.

Em conformidade com a adoção de um sistema elétrico do tipo *dual-bus* ou *three-bus*, torna-se aconselhável a implantação de duas ou três subestações independentes de média tensão contando com transformadores de aproximadamente 2,5MVA cada, a serem instalados em dois ou três locais distintos do prédio com entradas alimentando os quadros de média tensão contando com disjuntores de segurança. Estes quadros devem alimentar os transformadores de média tensão do tipo a seco, os quais visam rebaixar a tensão de 13.8kV para baixa tensão e alimentar via *bus-way* (barramentos) os quadros gerais de distribuição elétrica em baixa tensão em circuitos trifásicos instalados nas próprias subestações.

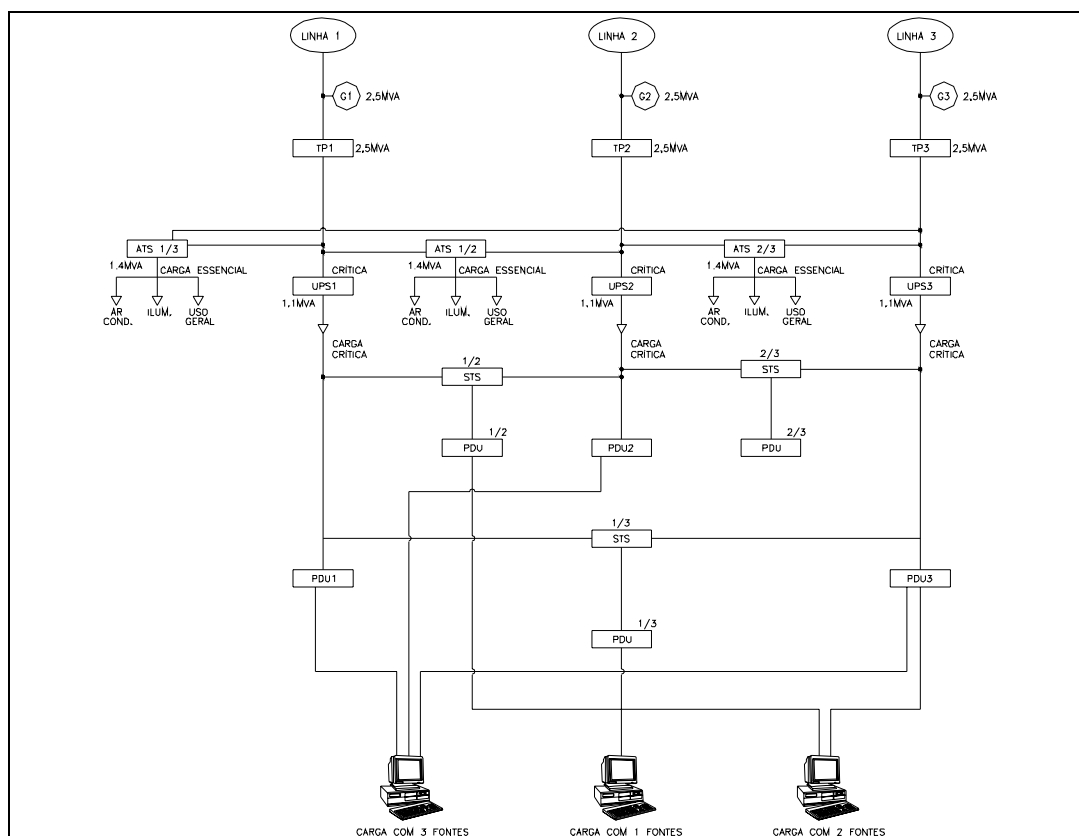
Cada subestação elétrica deve ter um sistema redundante de energia suportado por um conjunto de grupos motores geradores de capacidade individual que pode chegar em torno de 2,5MVA, sendo que a transferência automática deve ocorrer em média tensão com chave tipo ATS-*Automatic Transfer Switch*, equipada por sistema de *bypass* externo e facilidades para transferência a quente. As chaves de transferência (ATS) devem ser instaladas nas subestações de energia elétrica, com capacidades compatíveis ao sistema visando a transferência em média tensão das cargas totais do CPD.

Cada quadro de distribuição elétrica essencial, localizados em distintas subestações independentes, deve alimentar os sistemas UPS-*Uninterruptible Power System* e sistemas de ATS que visam possibilitar a conectividade entre as 2 (duas) ou 3 (três) linhas, sendo que cada uma destas deve alimentar suas cargas específicas de

retificadores, ar condicionado, iluminação e cargas de uso geral totalizando o montante de capacidade em cada linha. Nesta finalidade pode ocorrer o uso de ATS's de baixa tensão (480V), com sistema de *by-pass* externo e facilidades de transferência a quente. Por sua vez cada sistema UPS deve alimentar um quadro de ENERGIA CRÍTICA com capacidade total proporcional à máxima densidade de cargas a serem instaladas conforme projetado. Cada conjunto UPS contendo o banco de baterias, retificador e quadro de distribuição de energia crítica deve ser instalado em salas fisicamente separadas.

Cada quadro de energia crítica deve alimentar um conjunto de PDU-*Power Distribution Unit* (PDU A, PDU B ou PDU C) e as chaves estáticas de transferência STS-*Static Transfer Switch*. Cada PDU que pode ser de capacidade total em torno de 225KVA ou 300KVA e deve contar com transformador de entrada em baixa tensão em delta e saída de 208/120V em estrela com fator $K=20$ (obs: no transformador, trata-se do fator que determina o nível de atenuação de harmônicos) e aproximadamente 126 pólos divididos em três colunas de disjuntores, preparados para ligações monofásicas, bifásicas e trifásicas. Os PDU's devem ser instalados o mais próximo possível da carga crítica e assim evitar que os harmônicos influenciem em toda a distribuição elétrica. Cada ambiente de missão crítica terá um conjunto de PDU's compatíveis com a sua carga e redundâncias necessárias, podendo ainda contar com um último tipo de quadro de distribuição de energia crítica denominado de RPP-*Remote Power Panel* com alimentação derivada do PDU, a ser posicionado ainda mais próximo da carga crítica no ambiente de TI do CPD.

As STS's de maior capacidade e em baixa tensão, podem ser instaladas nas salas das respectivas UPS ou em corredores técnicos próximos às áreas de TI, ou ainda, podem ser de menores capacidades para instalações dentro dos PDU's, sendo que na elaboração do Projeto Conceitual do CPD estes detalhes devem ser solucionados. Como referência a Figura 25 na página seguinte demonstra um exemplo de diagrama elétrico em blocos de projeto básico com os primeiros estudos de dimensionamento para as cargas e equipamentos em um sistema típico de configuração *three-bus*.

Figura 25 – Exemplo de Diagrama Elétrico em Blocos*Fonte : SISTENGE*

As cargas essenciais tais como, ar condicionado, iluminação, retificadores e utilidades, devem ser alimentadas pela saída da ATS, que por sua vez deve ser alimentada por duas linhas do sistema, portanto, as cargas essenciais devem permanecer em operação mesmo com a queda de uma linha do sistema. Em casos de quedas simultâneas de 2 (duas) linhas do sistema, a linha remanescente não suportará 100% da carga essencial, sendo necessário a implantação de um sistema de rejeição de carga para este caso.

São recomendadas internacionalmente duas linhas independentes e de fornecedores distintos de energia elétrica, visando a alimentação das subestações elétricas de um ambiente de missão crítica, mesmo assim, os sistemas de geração de emergência devem ser interligados a cada linha de distribuição com o intuito de prover um sistema redundante de alta confiabilidade. Os transformadores de potência devem ser do tipo de isolamento a seco com uma tensão primária em média tensão (13.8kV) e um

secundário em baixa tensão. Devem ainda ser instaladas as chaves de transferência automática entre as fontes de energia principal e emergencial, chaves estas removíveis para manutenção e com “*by-pass*” de manutenção acoplado ao sistema (Quadro de Transferência automática com “*by-pass*” de manutenção).²⁷

Baseando-se na premissa de um sistema elétrico *three-bus* e adotando-se no projeto 03 (três) subestações elétricas independentes fisicamente, caso esta não seja a configuração possível por razões técnicas e de viabilidade econômica, o projeto conceitual do CPD deve considerar a construção de no mínimo 2 (duas) subestações, porém com 3 (três) interligações independentes até o último nível de distribuição em baixa tensão.

Cada subestação elétrica de média tensão (13,8 kV) deve contar com uma construção civil adequada, minimizando riscos de incêndio, explosão, inundação e acidentes externos, projetada para possuir ventilação natural e ter uma temperatura máxima ambiente de 40°C, sendo que em casos extremos podem ser utilizados um conjunto de dispositivos para a ventilação forçada. Ainda deve ter um quadro de média tensão com disjuntor extraível do tipo SF – 6 (gás isolante) ou a vácuo com facilidade para monitoração remota. Os transformadores em cada subestação devem ter entrada em configuração Delta em Média Tensão (13,8 kV) com saída de baixa tensão em configuração Estrela (Y), contando com sensores internos de temperatura nas bobinas, os quais em caso de sobreaquecimento devem enviar sinais para o disjuntor do quadro de média tensão visando o desligamento de energia.

Os Geradores de Emergência devem ser instalados para aumentar a disponibilidade de energia elétrica, visando reduzir as interrupções de energia para a carga crítica, pois eles substituem a fonte de energia principal em 10 à 30 segundos, tempo este suficiente para o sistema de baterias da UPS manter a carga crítica. O sistema de baterias deve ser projetado para uma autonomia de 15 à 25 minutos em carga total até que o gerador assuma toda a carga do CPD. O motor do gerador deve suportar temperaturas entre 80 e 185 °C, sendo que, deve ser provido um completo sistema de operação automático em eventos de interrupção da fonte principal de energia. Os

controles manuais devem prever a possibilidade de operar o sistema manualmente em eventos com problemas de controles automáticos e/ou necessidade, baseando-se na premissa de um sistema elétrico *three-bus*, há 03 (três) conjuntos de geradores, sendo 01 (um) para cada linha de alimentação.

Cada sala de geradores deve ter um tanque diário de combustível com capacidade máxima de 1.500 litros e com piscina de contenção para vazamento, devendo serem também instalados os tanques gerais de combustível com capacidade de autonomia adequada para alimentar os tanques de combustível diário em situação máxima de contingência. Estes tanques podem permitir uma autonomia de funcionamento superior à 30 (trinta) horas com carga total e serem instalados em áreas externas ao prédio do CPD, conforme legislação específica e detalhamento definido no projeto executivo. Estes tanques gerais podem ser instalados abaixo do solo (enterrado), com o intuito de se obter o maior índice de segurança possível e, caso seja possível, devem ser instalados em área que favoreça o fornecimento de combustível dos tanques gerais para os tanques diários por meio de gravidade. Em casos que o uso da gravidade fique prejudicada, deve ser instalado um sistema de bombeamento de combustível, sempre prevendo redundâncias. As tubulações de combustível entre os tanques gerais e os tanques diários devem ser de aço carbono, sendo que neste item também deve ser prevista a redundância.

As características básicas dos grupos geradores podem ser descritas conforme as necessidades do projeto, incluindo-se os seguintes detalhamentos exemplificativos : capacidade de carga em 2,5MVA; motor à diesel com 1800 rpm e radiador para resfriamento; regulador de voltagem que permita em cargas acima de 60% de capacidade do gerador, uma queda de tensão na transferência de no máximo +/- 7% da nominal, sendo que com 4 segundos após assumir a carga a variação de tensão esteja em +/- 2%; regulação estática em +/- 1% de variação na tensão de saída do gerador em carga; alternador em 13,8kV, 60 HZ e classe de isolamento F/H; regulador de frequência que permita com cargas acima de 68% da capacidade do gerador, a queda de velocidade se limitar em 10% da velocidade nominal e o retorno da velocidade em níveis de +/- 2% da nominal dar-se em no máximo 4 segundos após o

gerador assumir a carga; variação máxima de 1% da frequência nominal com gerador em carga; regulador eletrônico de frequência; painel de controle com instrumentos gerais contando com voltímetro, amperímetro (por fase), frequencímetro, horímetro, contador de ligações, medidas de temperaturas, medidas de pressão de óleo, voltímetro para bateria do sistema de ignição; controles que contenham chave seletora/ manual/ desligado/ automático, gerador ligado, desligado e teste, chave de desligamento remoto do gerador; alarmes gerais de pressão baixa de óleo, alta temperatura, sobre velocidade, falha de partida, sobrecarga, baixo nível de combustível; alarmes remotos que permitam sinalizar todos os alarmes anteriores e que devem estar disponíveis para serem visualizados/controlados por um sistema de gerenciamento remoto, portanto, o processador eletrônico da máquina deve possuir um software com protocolo aberto para troca de dados; os sistemas de geração de emergência devem ser projetados para suportar 90% de fator de demanda da carga total.³³

Conforme premissas de um sistema elétrico *three-bus*, o fornecimento de energia em média tensão deve contar com 03 (três) linhas independentes, portanto, se faz necessária a instalação ATS's de média tensão e de baixa tensão em cada linha, compatíveis com a capacidade total do sistema. A chave de transferência automática (ATS-*Automatic Transfer Switch*) deve contar com duas entradas (normal e emergência) e uma saída (essencial), sendo o nominal em média tensão para 13,8 kV e em baixa tensão para 480 V, podendo no projeto executivo serem modificadas estas tensões, após estudos de custos x benefícios.

A ATS em modo automático deve dispor de uma transferência de fontes de energia (A,B) com abertura de contato (A) antes do fechamento do contato (B), constituindo-se na categoria de transferência denominada de *BBM-Break Before Make*. Oferecendo facilidades eletrônicas para transferências manuais e programadas entre duas fontes de energia independentes, sem implicar em paralisações ou quedas de sistemas na carga crítica, esta função constitui-se em categoria conhecida como transferência a quente ou *MBB-Make Before Break*. A ATS deve ter um sistema de *by-pass* externo, visando possibilitar as transferências quando em manutenção da chave ou defeitos do automatismo. O sistema de transferência (chave mecânica, ou

disjuntores de média tensão do tipo a vácuo ou SF-6) deve ser do tipo removível, visando-se facilitar os serviços de manutenção.

Os bancos de capacitores são largamente aplicados em construções de Missão Crítica, sendo válidas muitas observações sobre este tipo de sistema, cuja instalação no sistema elétrico tem a função de corrigir o Fator de Potência (FP) do sistema causado por interferências de cargas reativas, indutivas e capacitivas presentes nos diversos componentes sistêmicos do complexo de equipamentos e instalações envolvidas no espaço construído do CPD. Tais dispositivos devem ser dimensionados com base na carga média em fator de potência 0.8, contando com os elementos que permitam manter um fator de potência de aproximadamente 0,95 para todo o sistema. Os bancos de capacitores devem ser compostos por vários capacitores individualmente chaveados, com um intuito de se permitir uma regulação do fator de potência geral do sistema elétrico. Este tópico, ao ser tratado no projeto executivo do CPD, deve considerar todo o dimensionamento e posicionamento dos dispositivos nos quadros gerais de energia, nunca prevendo-se aplicação diretamente instalada no gerador.

Os sistemas UPS-*Uninterruptible Power System* (no-break) não apenas fornecem energia de qualidade, mas também uma energia confiável, pois mantém na sua saída uma energia constante para a carga crítica, durante as interrupções da fonte de energia principal. O sistema UPS deve ser interligado a um banco de baterias para suprir a alimentação da carga crítica, quando a fonte de energia principal encontra-se fora de ação, sendo projetado para transferências via as baterias e de volta via a fonte de energia principal, sem causar impactos negativos ou quedas de energia para a carga crítica, constituindo-se um filtro absoluto que visa oferecer um excelente nível de energia com a máxima segurança aos equipamentos e funções de TI abrigados e suportados adequadamente no ambiente crítico do CPD.

A energia de alta qualidade somente pode ser fornecida pelo sistema de UPS *On-line* ou Dupla Conversão, no qual a carga crítica encontra-se completamente isolada da fonte de energia primária ou principal. O sistema de UPS *On-line* Estático fornece

uma energia qualificada e controlada, pela conversão do sinal senoidal de corrente alternada *AC-Alternate Current* (Corrente Alternada), da energia principal em sinal ou forma de onda de corrente contínua, *DC-Direct Current* (Corrente Contínua), e então regenera uma nova forma de onda AC usando a forma de onda DC. As baterias do sistema UPS são ligadas em paralelo formando bancos de baterias, que devem ser instalados em uma sala especial (sala de baterias).

A UPS *On-line* fornece a energia das baterias no fluxo para a carga crítica sem interrupção. Durante a operação normal do sistema, a regeneração da forma de onda AC, isola completamente a carga crítica de anomalias de qualidade de energia, provenientes da fonte de energia principal ou de emergência. Durante interrupções da fonte de energia principal, os bancos de baterias suportam a regeneração de corrente alternada, através de corrente contínua por um espaço de tempo limite de descarga de baterias geralmente entre 15 e 25 minutos. A voltagem e a frequência de saída são controladas e mantidas independentemente das condições de energia de entrada. O sistema de UPS *On-line* fornece energia extremamente confiável para a carga crítica, sendo chamados de *on-line*, porque todo o fluxo de energia através da UPS, para a carga crítica e o banco de baterias, devem estar conectados durante a operação normal do sistema.

Sistemas UPS *Off-line* tem operação similar ao sistema *on-line*, com a exceção de que todo o fluxo de energia não passa pela UPS durante a operação normal. Neste caso o fluxo de energia passa por um circuito “*by-pass*”, provendo uma conexão direta entre a fonte principal de energia e a carga crítica. Neste sistema, durante a operação normal não há uma regeneração do sinal, ou seja, a energia não pode ser purificada no processo de conversão de energias AC-DC. Durante interrupções da fonte principal de energia, o sistema UPS e baterias são chaveados para manter a operação contínua, assim, os sistemas *off-line* não são recomendados para aplicações de Missão Crítica para TI.

A existência de redundância nos sistemas UPS's pode resultar em economias quando o preço de um equipamento adicional requerido para configuração redundante, ao ser analisado frente à criticidade da carga e o custo causado por interrupções, concluir

que se justifique o custo x benefício desta redundância. Módulos redundantes não são instalados para proteger a carga crítica de falhas de fornecimento de energia principal, ao contrário, eles são instalados para manter o condicionamento ou qualidade e proteção da energia para carga crítica em eventos de falha de módulos de UPS's. Sem redundância, as falhas em módulos de UPS e as manutenções ou reparos de peças, requerem a transferência da carga crítica para uma energia não condicionada, não protegida e não qualificada, provenientes da rede pública de energia ou de sistemas de geração de emergência.

O mais direto e óbvio benefício da redundância pode ser o fato de a carga crítica continuar sendo alimentada pelo sistema UPS, mesmo quando um módulo for desconectado para serviços de manutenção e reparos. As características básicas dos sistemas UPS's podem ser descritas conforme as necessidades do projeto, incluindo-se os seguintes detalhamentos exemplificativos : capacidade composta em associações de módulos singelos para até 1,0MVA com 15 ou 20 minutos de autonomia das baterias; entrada AC em baixa tensão, trifásico com variação de tensão entre -10% e +15%; frequência de 60 Hz +/- 5% de variação admitida na entrada; saída AC em baixa tensão, trifásico com variação de tensão não superior a +/- 1%; frequência de 60Hz, +/- 1% de variação de saída; distorção harmônica na tensão igual ou menor a 3%, para carga linear na capacidade total; fator de crista: 3 (três); transiente de tensão em +/- 8% acima de 100% regulação da mudança de carga; sobrecarga : 150% durante 1 minuto, 125% durante 10 minutos; by-pass via chave estática e de manutenção; entrada DC de corrente máxima Ripple durante a flutuação da bateria em 2%; eficiência maior que 90% para a carga total; nível de ruído menor que 75 dBA à 1 (um) metro; botão de desligamento geral do equipamento, com previsão para desligamentos remotos; painel de monitoração com histórico de alarmes gerais, facilidade para monitoração e controle em um sistema remoto de gerenciamento de alarmes.³⁴

Uma folga extra de capacidade propicia facilidades para o sistema UPS absorver horários críticos de consumo e correntes de partida dos equipamentos, desbalanceamento de cargas e sobrecargas em uma fase, margem de segurança para

futuros crescimentos de projeto, bem como, a expectativa de vida do sistema e sua confiabilidade também são prolongadas substancialmente quando a carga está abaixo de sua máxima capacidade. O UPS apresenta-se altamente dependente das baterias aplicadas para gerar energia emergencial, assim, um extremo cuidado deve ser tomado na seleção, instalação e manutenção destas baterias, com um severo controle do ambiente onde se encontram.

As baterias devem ser dimensionadas visando permitir que a sua capacidade de depreciação seja maior que o seu tempo de vida, em geral, são universalmente garantidas para produzir 80% de sua inicial potência na saída, no final de tempo de vida. O tempo de duração de descargas e recargas tem um grande efeito no dimensionamento de um sistema de UPS, cuja duração de 15 à 25 minutos na descarga de bateria com carga total, normalmente se faz recomendado. Esta autonomia deve ser ampla e cuidadosamente estudada com o cliente e a equipe do projeto, com a premissa de que o CPD possa responder as expectativas operacionais desejadas.

As baterias chumbo-ácidas têm uma vida útil estimada em 20 anos, sendo muito mais econômicas quanto ao preço por KW, entretanto, emitem gás hidrogênio que tem a característica de ser potencialmente explosivo e insalubre, por este motivo, tem sido exigido um ambiente especial e enclausurado com um sistema especial de ventilação. Além disso, estas baterias ocupam muito espaço físico e exigem uma carga de laje maior em razão do peso elevado. Este tipo de bateria apenas deve ser recomendado para grandes construções, onde os espaços disponíveis são de maior capacidade e a manutenção adequada para suportar este tipo de sistema.

As baterias seladas reguladas a válvula têm uma vida útil em torno de cinco anos, em condições normais de operação, sem emissão de gases para o ambiente devido ao catalisador interno. No ambiente em que se encontram não se faz necessário nenhum tipo de tratamento, portanto, as baterias podem ser instaladas inclusive em salas de equipamentos de TI. Apesar de requerer um maior número de elementos e conexões para produzir o mesmo KW que os elementos das baterias chumbo-ácidas, os elementos das baterias reguladas a válvula podem ser acondicionados

horizontalmente, logo, torna-se possível construir bancos verticais com vários elementos acondicionados horizontalmente, reduzindo assim muito do espaço requerido para a instalação. Este tipo de bateria requer uma rotina de manutenção extremamente reduzida se comparadas com as chumbo-ácidas, portanto, as baterias seladas reguladas a válvula são as mais indicadas para o ambiente crítico de CPD.

A infra-estrutura do CPD deve ser toda preparada para receber, trocar, retirar e substituir equipamentos sem que os ativos e funções de TI sejam impactados negativamente, assim sendo, a redundância do sistema de distribuição de energia *dual-bus* ou *three-bus* deve ser desenhada visando fornecer energia para o CPD sem quaisquer interrupções em períodos de manutenções preditiva, preventiva e corretiva em Geradores, UPS's, ATS, STS e painéis de distribuição. Os painéis elétricos dedicados que devem alimentar os sistemas de ar condicionado de precisão devem ser supridos alternadamente no mínimo por 02 (duas) linhas distintas de alimentação.

No ambiente interno do CPD há dois tipos distintos de alimentadores no sistema elétrico, um proveniente de UPS e outro proveniente de um sistema sem a proteção especial via no-break, propícios para usos gerais, como, por exemplo, tomadas para ligar ferro de solda, equipamentos de limpeza, furadeira etc. Estes alimentadores devem ter identificação distinta, ou seja, uma cor para tomadas protegidas e outra cor para tomadas de uso geral. Tanto os circuitos protegidos quanto os de uso geral, devem ser disponibilizados nas tensões 120 volts (FNT) e 208 volts (2FT e 3FT), também com suas respectivas identificações.

O painel de distribuição e os painéis auxiliares devem ter barras isoladas de terra, conforme as normas de aterramento para os equipamentos eletrônicos sensíveis, mediante isolação adequada à voltagem de trabalho e devem ser do tipo armário conjugado com portas para visualização e manutenções internas. Também devem ter facilidade para entrada/saída de cabos de energia ou *bus-way* (barramentos), tanto na parte superior como na inferior do quadro. Disjuntores de alta confiabilidade, com capacidade suficiente de curto-circuito e com dispositivos de desligamento (*trip*)

eletro-magnético regulável, devem ser utilizados, sendo que, os disjuntores principais devem possuir dispositivos auxiliares para a telesinalização de estado e de atuação, podendo ser analisada a inclusão de bobinas de disparo, para atuação remota (exemplo: em caso de inundação de sprinklers e outros).

As interligações elétricas (físicas) dentro dos quadros elétricos, devem ser de barramento em cobre, com dimensões tais para suportarem as tensões e correntes de trabalho/curto-circuito do sistema. Os quadros devem ser equipados com instrumentos digitais para o completo controle de funcionamento, através de diversos meios para medidas elétricas, tais como : voltímetro (RS, RT, ST, RN, SN e TN); amperímetro com medições de correntes em cada fase; wattímetro; medidores eletrônicos com CPU são muito utilizados em instalações *high-tech*, pois eles podem enviar todos os dados e medidas atuais e históricas, para um sistema de gerenciamento remoto, sendo portanto, o modelo mais recomendado para ser instalado em um ambiente de CPD; relés de proteção de sobre-corrente e sobre/subtensão eletrônicos com CPU são recomendadas para este sistema, porém, eles somente podem ser instalados antes dos sistemas UPS, caso contrário, o seu sistema de *trip* pode desligar a carga crítica do CPD. Os disjuntores principais de cada quadro devem ser do tipo removível e com facilidade para ajuste de seletividade. Os cabos ou barramentos interligados aos disjuntores devem ter espaço suficiente para permitir o uso de alicates amperímetros e outros medidores externos que devem ser utilizados em manutenções. Todos os disjuntores, chaves, barramentos, cabos, instrumentos e terminais devem estar em conformidade com o desenho disponível projetado. Uma cópia do desenho ou projeto do painel de distribuição deve ser disponibilizado em suporte no interior da porta do painel. Os quadros elétricos de distribuição devem ser instalados em bases metálicas ou de alvenaria ou ainda sobre tapete isolante de borracha ou equivalente, como também as UPS e os racks de baterias.³⁵

A PDU-*Power Distribution Unit* responsável pela distribuição de energia crítica aos equipamentos de TI, deve ser constituída por transformador e disjuntores de distribuição em um único painel e pode ser instalada em qualquer lugar do CPD. O

custo do investimento inicial em PDU's normalmente maior que os de painéis padrões montados, apresentam muitas vantagens quando em análises do ciclo de vida útil do sistema, como se pode observar pelo que segue : as PDU's são facilmente deslocadas o que aumenta a flexibilidade de lay-out no CPD; o transformador interno permite uma maior proximidade da carga crítica possibilitando a maximização de economia de alimentação e minimização de distorções harmônicas; as PDU's são facilmente interligadas ao sistema de referência de terra com uma pequena distância de cabo; possuem chave de desligamento de emergência e capacidade de monitoramento local e remoto; possibilitam monitoração completa de energia sendo estes opcionais oferecidos por muitos fabricantes; vem equipadas com um, dois ou até cinco painéis, cada painel com um disjuntor geral. Em face das vantagens detalhadas acima, alta qualidade de conexão e disjuntores (monofásico, bifásico e trifásico) removíveis a quente ("plug-in"), as PDU's são altamente recomendadas para ambientes de CPD.

De um modo geral a energia crítica deve ser suprida aos equipamentos de Tecnologia da Informação (TI) através de cabos flexíveis sob o piso elevado, sendo raramente utilizados os cabos rígidos, cuja técnica não deve ser recomendada, com exceções onde as normas locais exigem este material. A configuração dos equipamentos de TI deve determinar o comprimento, a dimensão ou bitola e o tipo de cada cabo. As cargas críticas com duas fontes devem ser alimentadas por duas PDU's distintas, sendo as cargas de única fonte alimentadas por uma PDU que recebe alimentação de um sistema de STS-*Static Transfer Switch*, o qual deve receber as alimentações independentes provenientes das duas linhas do sistema elétrico.

Com estes modelos de ligações as cargas críticas podem sempre ter disponibilidade de alimentação de qualquer uma das linhas do sistema. Os cabos flexíveis devem sair dos disjuntores nas PDU's e serem encaminhados sobre canaletas do sistema elétrico sob o piso elevado, a serem interligados em tomadas elétricas do tipo industrial com trava de segurança ou caixas de conexões seguras com tampa transparente para a visualização em *check-list* das condições de funcionamento.

As STS-*Static Transfer Switch* possuem características importantes, cujo desempenho nas manobras de transferência automática por ocasião de falhas nas unidades UPS deve ser capaz de produzir um movimento quase instantâneo com tempo menor a 4 (quatro) milissegundos, além de ter a disponibilidade para configuração de transferência automática reversa, com 15 segundos de atraso antes da retransferência, bem como, a configuração para transferências não sincronizadas em tempos mínimos de interrupção. As características de desvio de fase, sobre/subtensão da STS devem ser compatíveis com as características das cargas críticas, sendo que, os disjuntores sem perda residual de corrente também devem ser instalados após o sistema STS, podendo ser avaliada a opção de instalação de STS's internamente nas PDU's.

A instalação de um sistema TVSS-*Transient Voltage Surge Supression* se faz recomendada para ambientes de CPD, mediante um conjunto mínimo de dispositivos TVSS que devem ser instalados em cada equipamento, na entrada geral de energia e painéis de distribuição que alimentam os equipamentos eletrônicos sensíveis. O TVSS no painel de entrada (subestação) visa eliminar picos de voltagem e transientes vindos da rede comercial. O TVSS no painel de distribuição visa atenuar transientes e ruídos que são gerados internamente nos prédios. O equipamento TVSS pode ser equipado com contadores de transientes e fusíveis indicadores de ação rápida que podem ser interligados ao sistema de automação predial para enviar informações e alarmes. As características básicas dos equipamentos TVSS podem ser descritas conforme as necessidades do projeto, incluindo-se os seguintes detalhamentos exemplificativos : baixa tensão a ser definida oportunamente; taxa de transiente de corrente (8 a 20 microssegundos) $>$ ou $= 10 \text{ KA}$; pulso máximo único de transiente de corrente $>$ ou $= 20 \text{ KA}$ (8 a 20 micro segundos); supressão dinâmica de voltagem na taxa de corrente $<$ ou $= 2 \text{ KV}$ (fase para terra); tempo de resposta de 50 nano-segundos; regenerativo; tecnologia com circuitos híbridos; indicador de falhas; deve ser instalado o mais próximo da saída do disjuntor principal, de modo que não interrompa os circuitos elétricos; dispositivo de proteção com chave seca + neutro conectados ao terra, em cabo de bitola mínima 4 mm^2 .^{2, 34}

Os cabos de energia e os cabos de lógica (dados) devem ser instalados em bandejas distintas e separadas visando minimizar os riscos de interferência eletromagnética. Existem construções que se utilizam de bandejas para cabos de energia sob o piso elevado e bandejas para cabos de lógica (dados) em sistema fixados no teto através de leitos aéreos no CPD. A opção desta solução ou da solução de todas as bandejas posicionadas sob o piso elevado, constitui-se tomada de decisão a ser efetuada pelo cliente, pois quaisquer destas soluções são exeqüíveis no tocante técnico e construtivo. As bandejas devem ser de aço galvanizado, sem nenhuma superfície cortante em toda a sua dimensão. As bandejas devem estar no mínimo 03 (três) cm acima do contrapiso sob o piso elevado e toda sua estrutura deve estar conectada ao terra nas 02 (duas) extremidades. As emendas devem possuir interligação elétrica que assegure a continuidade elétrica independente das conexões físicas.

Os cabos e fios de energia em geral devem ser do tipo PVC ou XLPE com níveis de isolamento apropriada para cada área do CPD, sendo que, os que são posicionados em *shafts* devem ter proteção contra incêndio para 60 minutos. Todos os cabos e fios elétricos (fases, neutro e terra), devem ter códigos de cores identificando os mesmos. Estas cores podem estar na própria isolamento de PVC do cabo, ou cabos com uma única cor de isolamento, identificados com fitas coloridas coladas no mesmo, e ainda, devem ser identificados com anilhas indicativas de circuitos, conforme determinado no projeto executivo.

As boas práticas de aterramento são essenciais para uma confiabilidade dos sistemas críticos e todas as separações derivadas de fontes – sistema de UPS's, transformadores e geradores – devem ser obrigatoriamente interligadas ao sistema de aterramento com eletrodos. Em adição, o sistema de aterramento deve estar totalmente interligado, ou seja, sistema de proteção contra descargas atmosféricas (para-raios) e os sistemas equipotenciais de aterramento devem estar obrigatoriamente conectados ao sistema de eletrodos. Os sistemas de aterramento para equipamentos de missão crítica, geralmente consistem nos seguintes subsistemas: aterramento para segurança de equipamento; aterramento isolado; aterramento equipotencial.

O aterramento para segurança de equipamento refere-se no código de cores ao condutor estabelecido como verde para a indicação do terra, sendo requisitado para a proteção contra curto-circuito, mas geralmente não serve bem como uma referência de sinal ou supressão de ruído no terra. O cabo verde do terra pode ser dimensionado em bitola igual ou dobro dos cabos de fase no circuito de 120/208 volts que alimentam os equipamentos de tecnologia. Muitos equipamentos de alta tecnologia são manufaturados podendo requisitar aterramento isolado ou sistema de aterramento de referência de sinal. Na atualidade, os sistemas de aterramento não apresentam a condição de serem totalmente isolados e o melhor que se pode obter é um aterramento limpo. Aterramentos limpos não podem ser divididos em algum ponto em comum com algum outro sistema, exceto o ponto do terra ou o ponto do neutro aterrado, sendo que, ele consiste de barras isoladas de terra e cabos convergindo para um ponto único de aterramento equipotencial. Com o intuito de manter um sistema potencial com terra isolado mais próximo possível de outro sistema de aterramento, torna-se essencial a execução de um sistema de neutro aterrado para servir a área de Missão Crítica, como no sistema UPS onde o seu neutro pode ser interligado ao ponto equipotencial de aterramento. O uso do sistema equipotencial de aterramento instalado abaixo do piso elevado pode ser recomendado para os ambientes de CPD. Este sistema provê um plano equipotencial de terra, que aumenta a atenuação de ruídos e pode ter um condutor de perímetro, interligado a várias fitas de cobre tratadas formando uma grande cadeia por baixo de todo o piso elevado, provendo uma grande uniformidade equipotencial. O sistema equipotencial deve ser interligado a ponto de neutro aterrado da subestação do prédio, com o intuito de manter o mesmo potencial do aterramento de segurança. Os sistemas de neutros separados derivados dos equipamentos de infra-estrutura, como o secundário do transformador do PDU, devem ser interligados ao plano equipotencial e o dimensionamento deste sistema deve ser objeto do projeto executivo.³⁶

Alguns equipamentos de missão crítica requerem uma alimentação DC (-48V), nestes casos devem ser instaladas as fontes de energia DC que consistem em uma planta primária com redundância. Este sistema DC possui várias unidades

retificadoras com filosofia de redundância e um banco de baterias projetado para um tempo de descarga (autonomia) que pode ser de 10 horas com carga total. O próprio painel do sistema DC deve ter um quadro com disjuntores para distribuição de energia e ter facilidade para instalação de um quadro remoto de distribuição DC, sendo que, o dimensionamento deste deve ser objeto do projeto executivo.

Enfim, o quadro resumo de requisitos para a Infra-estrutura Elétrica do CPD compreende os conceitos e premissas básicas do Fornecimento e Distribuição de Energia que abrangem os seguintes tópicos relacionados a seguir :

- i. Disponibilidade de energia, com e sem interrupção;
- ii. Qualidade de energia – aterramento, supressão de surtos, filtragem, compatibilidade eletromagnética;
- iii. Adaptabilidade – modularidade, estrutura do cabeamento;
- iv. Proteção física e elétrica dos sistemas de energia;
- v. Monitoramento, Detecção, Manutenção e Gerenciamento.

4.3 Climatização, Ventilação e Resfriamento

Neste tópico são abordadas as necessidades de remoção do calor dissipado nos ambientes de sistemas e sua infra-estrutura, onde a premissa básica para todos os elementos refere-se a disponibilidade 24x7 (24 horas por dia, 07 dias por semana e 365 dias por ano) em todas as áreas de TI. Os ambientes da “Cabine de Comando” (*CC-Comand Center*, *NOC-Network Operation Center*, *SOC-Security Operation Center*) requerem climatização com características mistas de conforto e concentrações de equipamento dissipando calor sensível. Os ambientes de subestações elétricas requerem dispositivos de exaustão e os ambientes de geradores requerem sistemas de arrefecimento específicos a serem projetados na fase executiva.

O ambiente para o CPD propriamente dito, considerando-se sob enfoque principal as áreas dos equipamentos de TI, pode ser objeto de avaliações de, no mínimo, duas alternativas técnicas para a remoção de calor dos ambientes de sistemas – alternativa com água gelada e alternativa por sistemas distribuídos, sendo que, as outras alternativas podem ser desconsideradas em função das necessidades de flexibilidade e segurança (ex: centrífugas, absorção, geotérmica, torre de água, etc).

Na alternativa com água gelada, o resfriamento deve ser efetuado em planta central com temperatura inferior a 10°C e o circuito de água fria deve passar por unidades de troca de calor nos ambientes. A configuração do sistema com água gelada, deve considerar uma composição por dois, três ou mais chillers constituindo uma planta termo-mecânica, resfriando circuitos fechados de água. O calor deste processo deve ser descarregado no ar. A água deve circular em tubulações isoladas até chegar em todos os ambientes que devem ser resfriados. Os ambientes dos equipamentos e funções de TI devem ser climatizados por unidades Fan-Coil de Precisão (troca de calor ar-água com ventilação forçada), complementadas com umidificador e aquecedor para correção da umidade. As vantagens do sistema com água gelada levam em consideração a manutenção da planta termo-mecânica que fica centralizada e fora dos ambientes dos computadores (a manutenção das unidades fan-coil, dentro dos ambientes, continua indispensável) e permite a aplicação do conceito de termo-acumulação para cortar picos de demanda. As desvantagens do sistema com água gelada levam em consideração a possibilidade de redundância dos circuitos de água em cada ambiente que não passa de 1+1, o que demanda dois grupos de Fan-Coils (N+N) ou um complexo sistema de interligação hidráulica, para permitir a redundância no equipamento e na linha, sendo que a paralisação de um dos circuitos deixaria os sistemas sem redundância e há riscos inerentes da grande quantidade de água em circulação nos ambientes de Missão Crítica, além de que, a água demanda manutenção química, as unidades da planta central são de grande porte, portanto a modularidade não permite ajuste fino e o atendimento sob medida com unidades no estoque (*on demand*), não há recuperação do investimento da planta central em caso de redução da demanda (menor proteção do investimento), a arquitetura tem que oferecer um local com facilidade da descarga do calor e com segurança adequada

para a planta central, o sistema de controle pode ser complexo (local e central) com integração específica do projeto (não sendo *plug & play* de fábrica), a alteração no sistema de controle requer serviço de engenharia e as grandes cargas do sistema central dificultam a provisão de redundância na alimentação de energia.

Na alternativa por sistemas distribuídos os sistemas são de pequeno porte, com circuito termo-mecânico autônomo (*self-contained* de precisão com condensador remoto) denominados de “expansão direta”, com absorção de calor pelo próprio gás refrigerante dentro do ambiente e descarga do calor em condensador ao ar livre. A configuração com sistemas distribuídos apresenta composição por módulos autônomos, compressor e evaporador no ambiente, circuito de gás / líquido até um condensador e descarga do calor na cobertura. As vantagens dos sistemas distribuídos são a independência e autonomia – não há função centralizada, os riscos são pulverizados e distribuídos, torna-se fácil conceber um sistema redundante de energia para garantir a operação, a redundância pode ser modular em cada ambiente que pode ter a configuração ideal de N+1, N+2 ou mais, um novo módulo pode ser instalado rapidamente (de 2 a 3 dias), o sistema de controle também pode ser modular em cada unidade que possui uma eletrônica embarcada testada em fábrica, a configuração dos conjuntos não requer engenharia especializada, os módulos podem ser adquiridos de acordo com a demanda (obs: em caso de redução da demanda torna-se fácil reutilizar em outros locais), o remanejamento pode ser simples com tubulação fácil de soldar e isolar, a padronização dos módulos permite grande agilidade na manutenção, sendo os impactos na arquitetura do prédio decorrentes apenas das prumadas de tubulações e a grande quantidade de condensadores. As desvantagens com sistemas distribuídos são o fato de que há um pouco mais de manutenção (obs: portanto, um maior fluxo de pessoas dentro dos ambientes de computadores), a grande quantidade de condensadores requer local seguro para rejeição de calor de preferência na cobertura e a limitação entre as distâncias evaporador-condensador que pode representar problemas em alguns casos.

Assim, a conclusão sobre o tipo de sistema mais adequado ao CPD deve considerar a alternativa de sistema (central ou distribuído) que possa oferecer mais vantagens por

um custo total operacional e aquisitivo igual ou inferior ao da tecnologia comparada, considerando-se todo o quadro resumo de vantagens e desvantagens apresentadas, mediante análise geral do “Custo do Ciclo de Vida” ou *LCC-Life Cycle Cost* dentre todas as alternativas consideradas no projeto conceitual do CPD. O critério de condições ambientais, internas e externas para dimensionamento das condensadoras deve adotar a temperatura máxima externa de 40 °C a 800 m acima do mar, com provisão para instalação de difusão de água sob os condensadores caso seja vantajoso para o sistema. Os ambientes de processamento demandam normalmente um ponto de ajuste em 21 °C para possibilitar o insuflamento a 15 °C, sendo o fluxo de ar ajustado para minimizar a demanda de correção da umidade, já que representa desperdício de energia. Salas de UPS devem seguir os mesmos critérios dos ambientes de processamento. Os ambientes de “Cabine de Comando” demandam condições de conforto com ajustes individuais para atender a grande variedade de ocupação por pessoas e concentrações locais de equipamentos de considerável dissipação térmica. Os índices a serem utilizados para os projetos executivos devem considerar as referências para as condições típicas de cada região, prevendo-se proteção contra infiltração mediante isolamento de todos os vãos de comunicação dos recintos condicionados com o exterior a serem mantidos em modo normalmente fechados.

A concepção e dimensionamento dos sistemas de climatização, ventilação e resfriamento deve considerar uma série de parâmetros de acordo com o tipo de ambiente a ser tratado, tais como : processamento, armazenamento e telecomunicações; ambientes de infra-estrutura física; ambientes de conforto com predominância de pessoas.³⁷

Nos ambientes de processamento, armazenamento e telecomunicações os compartimentos devem ser climatizados individualmente, em circuitos internos, por sistemas em configuração modular com redundância, de precisão, com alta vazão, alto teor de calor sensível, controle de umidade e filtragem eficiente. A capacidade inicial não precisa atender projeções futuras e as unidades podem ser acrescidas ou retiradas sem interferência na operação. A instalação deve incluir providências para

facilitar acréscimos futuros de unidades. A climatização segregada oferece grande adaptabilidade e previne que qualquer contaminação (fator constante na área metropolitana) ou subprodutos de um incêndio (fumaça, gases corrosivos, calor) possa penetrar no ambiente crítico via dutos de ar. A premissa básica deve ser a de que cada ambiente pode requerer uma configuração específica, não permanente no tempo. As cargas térmicas em sua grande maioria são todas “sensíveis”, ou seja, sem geração de umidade. Um ambiente de fitoteca robotizada pode apresentar demanda inferior a $200 \text{ W} / \text{m}^2$, enquanto uma área de servidores em racks altos pode passar de $1000 \text{ W} / \text{m}^2$ acrescentando problemas com ar quente de um rack ser aspirado por outro. A redundância de unidades precisa atender todas as previsões, inclusive reconfigurações e outras situações transitórias. Todas as unidades de climatização devem ser do tipo “precisão” ou “alta performance” com sofisticada eletrônica embarcada, as quais dependem da disponibilidade da energia essencial, alimentadas por gerador em caso de falta da energia comercial. Esta transferência deve ser automática e as partidas das unidades devem ser escalonadas e comandadas pelo próprio sistema de controle. As unidades devem possuir controles microprocessados autônomos incorporados na própria máquina e interligados em rede. O sistema pode manter uma ou mais unidades em *stand-by*, de acordo com a demanda, alternando sua operação sempre que algum alarme requerer. O insuflamento deve ocorrer diretamente sob o piso elevado com o retorno pelo ambiente, via filtro na parte superior da máquina. A descarga do calor de cada unidade deve ser por condensador remoto, resfriado a ar forçado com controle de rotação variável, localizado sobre a cobertura, quando se optar por sistema de self-ar. O controle de umidade pode ser facilitado pela estanqueidade dos ambientes, mas a estratificação térmica ser muito acentuada com conseqüente variação ainda maior da umidade relativa, mas sem alteração do teor absoluto. A estimativa da quantidade adequada de módulos para atender os ambientes previstos pode partir da demanda total de energia crítica (UPS), sendo que a soma das capacidades de calor sensível dos sistemas não deve ser inferior a 1,5 vezes esta demanda, o que significa redundância média de 50 %, o mínimo aceitável. Ambientes pequenos podem ter configuração mínima de 1+1, portanto 100 % de redundância. Com base no estudo da demanda atual do CPD, a ser estimada visando estabelecer a capacidade total em TR's, pode ser estabelecida a

quantidade necessária aproximada de unidades de selfs requeridas para atender uma eventual aplicação para novas construções de ambientes para Missão Crítica. Esta quantidade pode ser alterada a partir do projeto conceitual e o refinamento do projeto executivo do CPD. O layout do hardware e corredores determina a configuração ideal das unidades, sendo que a eventual obstrução do fluxo de retorno também pode criar *hot-spots* (pontos de aquecimento).³⁸

Nos ambientes de infra-estrutura física as UPS's e baterias representam funções críticas que dissipam calor sensível e sofrem redução de vida útil com elevação da temperatura a partir de 24 °C. As vantagens na padronização de equipamentos pode facilitar a opção pelo uso de sistema idêntico nestes ambientes. Um sistema de exaustão automática deve ser indicado para baterias que exalam gases, nos casos em que estas baterias sejam adotadas.

Nos ambientes de conforto (predominância de pessoas), visando climatizar as áreas de trabalho com equipamentos em configurações altamente dinâmicas, o sistema também pode ser modular e adaptável para atender os equipamentos e proporcionar conforto às pessoas no ambiente de trabalho, contando com a flexibilidade de layout. Para tanto, pode ser adotada a climatização sob o piso elevado com unidades terminais em forma de placa de piso com ventilador e grelhas para insuflamento. O retorno pode ser via *plenum* no entreferro, ou diretamente pelo ambiente, gerado pela diferença de pressão. Nesta área pode ser prevista a renovação de ar, devidamente filtrado, atendendo a norma NBR 6401, a Portaria No 3.523 de 28.08.1998 e o Regulamento Técnico RE09 de 16 de janeiro de 2003 do Ministério da Saúde. A recepção do CPD deve ser suprida por sistemas de conforto junto com a “Cabine de Comando”.³⁹

Os ambientes comuns de corredores e espaços para cabeamento, horizontal e vertical, não precisam de climatização. As especificações de equipamentos do sistema adotado devem descrever todas as características requeridas na aplicação sob enfoque, segundo as análises desenvolvidas em fase de projeto conceitual do CPD. As características básicas de um sistema modular de precisão para ambientes de TI e

de UPS podem ser descritas conforme as necessidades do projeto, incluindo-se os seguintes detalhamentos exemplificativos : a capacidade da unidade deve ser padronizada para obter modularidade e facilidade na manutenção; o módulo básico ideal deve possuir um só circuito termo-mecânico com capacidade de 20 a 30 kW de calor sensível; a relação (capacidade térmica) / (área ocupada) deve superar 20 kW / m² e as conexões de energia e de tubulação devem ser pela base, via entrespaço; toda a manutenção deve ser efetuada apenas pela área frontal, permitindo instalação em conjunto; visando permitir uma maior modularidade de projeto, facilidade de remanejamento futuro, alimentação elétrica e estoque de peças sobressalentes para agilização na manutenção, se faz recomendável que os equipamentos de precisão de toda a instalação sejam dimensionados utilizando-se no máximo 2 capacidades distintas, sem prejuízo da redundância já comentada; adoção de um número de condicionadores de ar por ambiente que permita utilizar uma distribuição homogênea das cargas de equipamentos de ar no sistema elétrico e aumentar a confiabilidade do sistema; as unidades devem fornecer o ar-condicionado diretamente ao entrespaço com pressão estática superior a 100 MPa através de ventilador centrífugo de pás curvadas para trás, acoplada diretamente (sem correias) a motor assíncrono de rotor externo; o ar quente de retorno deve ser aspirado pelo lado superior da unidade, passando por um filtro descartável de eficiência EU4 (ASHRAE 20-30 %); o compressor deve ser tipo scroll e o meio refrigerante deve ter ODP = 0 (sem efeito contra camada de ozônio); o evaporador deve possuir fator sensível superior a 90%; o gabinete deve ser fechado por sanduíche termo-acústico e as bandejas, parafusos e ferragens devem ser de inox; a desumidificação do ar ambiente, a ser feita através de reaquecimento, pode ser do tipo elétrico, de baixa temperatura superficial; a umidificação deve ser feita por um sistema autônomo de evaporação e aspersão de água por aquecimento elétrico, utilizando-se recipientes lacrados instalados no interior das unidades, que são substituíveis em caso de defeito (tipo “descartável”); o sistema de controle operacional deve ser uma rede configurada pelos microprocessadores embarcados nas unidades; cada unidade deve ter processador independente com visor, menu, teclas de navegação, *leds* indicadores de *status*, alarmes e proteção por senha; o sistema de controle operacional deverá possuir circuito eletrônico com auto-diagnóstico para auxiliar na identificação de problemas; o microprocessador do

sistema de controle, deve ser compatível com todos os dispositivos remotos de monitoramento e controle, com processamento do tipo avançado, com um mostrador frontal em cristal líquido, para indicar a temperatura, umidade, capacidade percentual (refrigeração, aquecimento, umidificação, desumidificação e ciclo de economia), *set point* (ponto de ajuste) de regulagens e sensibilidade de temperatura e de umidade; os alarmes, além de serem reportados à Cabine de Comando e ao Setor de Contrôlo da Infra-estrutura, devem ativar um alarme sonoro e visual na tela de cristal líquido da respectiva unidade, na ocorrência de qualquer uma das seguintes condições - Alta Temperatura/Alta Umidade/Baixa Umidade/Alta Pressão no Circuito Frigorífico /Problema com o Umidificador/Perda de Fluxo de Ar/Presença de água sob o piso elevado/Substituição de Filtros; a tubulação frigorígena deve ser de cobre soldada em atmosfera inerte, com fixações apropriadas para dilatação, isolamento térmico e proteção mecânica nos trechos indicados; a tubulação de água deve possuir registro externo ao ambiente, ser de cobre rígido, inclusive a de drenagem.⁴⁰

As características básicas de um sistema modular de conforto para ambientes do CPD com predominância de pessoas podem ser descritas conforme as necessidades do projeto, incluindo-se os seguintes detalhamentos exemplificativos : a solução precisa proporcionar conforto para ambientes tão diversos como os anfiteatros de operadores, salas de reunião de crise, sala de recepção vip, alguns ambientes para equipamentos sensíveis e ainda permitir reconfigurações drásticas na utilização do espaço, com o mínimo de interrupções em operações críticas; a climatização via piso elevado pode ser um conceito sustentável neste caso; podem ser aplicados os sistemas de 10 a 20 kW tipo *split* (com unidades condensadoras na cobertura e evaporadoras no local) fornecendo ar renovado, filtrado e resfriado sob o piso elevado; cada ambiente pode ser provido de terminais móveis, acoplados a uma placa do piso, com a função de climatizar uma área de 5 a 10 m², insuflando ar de acordo com a necessidade local; as grelhas do piso elevado devem ter capacidade adequada para distribuir o fluxo de ar na quantidade exigida pelo ambiente; as unidades de ar condicionado devem ser instaladas sobre estruturas metálicas acima do piso elevado, com pés de borracha para eliminar vibrações mecânicas; recomenda-se a instalação de dutos defletores sob o piso elevado, na saída das unidades de ar condicionado,

com o intuito de aumentar a eficiência da saída do fluxo de ar gelado das máquinas; as unidades de ar condicionado não devem ser instaladas próximas umas das outras, visando aumentar a eficiência de todo o sistema; as unidades condensadoras deverão ser instaladas na cobertura do prédio, em locais seguros, com facilidade para troca de calor, acesso adequado para manutenções e distante de exaustores de fumaça; o sistema microprocessado deve disponibilizar todos os alarmes para um sistema de gerenciamento remoto para que os operadores treinados possam atuar preventivamente a possíveis problemas do sistema de ar condicionado, ventilação e exaustão; o sistema de exaustão deve ter capacidade de troca total do ar do ambiente em 10 (dez) minutos, para a eventualidade de ocorrência de gás ou fumaça no ambiente, sendo que, este dispositivo deve ser instalado em ambiente externo à sala de operação com circuitos de proteção de operação acidental; os dutos separados entre as salas de operação e equipamentos, com dumpers devem ser interligados ao sistema de exaustão; todos os sistemas de climatização, ventilação e resfriamento deverão ser alimentados pela energia essencial e distribuídos igualmente entre as linhas de fornecimento do sistema elétrico com múltiplos barramentos (*dual-bus* ou *three-bus*); o sistema de exaustão não pode ser desligado pelo acionamento do sistema de detecção de incêndio, sendo que em casos extremos de necessidade de renovação de ar pode ser aconselhada a abertura das portas das salas de equipamentos e operação em conjunto com o sistema de exaustão forçada.⁴¹

Enfim, o quadro resumo de requisitos para a Infra-estrutura de Ar-condicionado do CPD compreende os conceitos e premissas básicas de climatização, ventilação e resfriamento que abragem os seguintes tópicos relacionados a seguir :

- i. Cada ambiente deve ter climatização própria, sem mistura de ar com outros, assim eliminando riscos de contaminação;
- ii. Cada ambiente precisa ter a redundância adequada, igual ou maior que N+1;
- iii. Cada módulo deve ser independente, sem vínculos de componentes em comum, nem de qualquer infra-estrutura do prédio com exceção da energia;
- iv. A capacidade inicial não precisa atender projeções futuras;
- v. Unidades podem ser acrescidas ou retiradas sem interferência na operação.

4.4 Segurança Física

Os sistemas de Segurança Física que devem ser previstos no projeto do CPD, assim entendidos todos aqueles sistemas cuja função seja monitorar, controlar e impedir que um evento fortuito venha a causar paralisação, falha de operação ou perda de informação do cliente, em uma instalação de alta disponibilidade podem ser divididos nas seguintes categorias de sistemas – Segurança Patrimonial; Proteção e Alarme de Incêndio; Segurança Operacional de Infra-estrutura.

A Segurança Patrimonial engloba os subsistemas de controle de acesso, detecção de intrusão, monitoração e tratamento de imagens e sistemas antifurto. A Proteção e alarme de Incêndio compreende as subdivisões de sistemas de detecção de incêndio precoce, sistemas de detecção de incêndio pontual, sistemas de extinção de incêndio e sistemas acessórios. A Segurança Operacional de Infra-estrutura abrange os componentes para detecção de líquidos e vapores, interferências eletromagnéticas, botões de desligamento e proteção contra descargas atmosféricas.

Todos os sistemas de Segurança devem possuir interfaces que permitam sua interligação ao sistema de Supervisão e Inteligência Predial, possibilitando o monitoramento dos parâmetros essenciais, acionando alarmes em caso de ocorrência de desvios ou eventos que possam colocar em risco a segurança ou operação do CPD. Além disso, deve ser previsto no desenho de layout da edificação uma sala específica de Segurança para abrigar o corpo de vigilantes, na qual devem ser instalados os equipamentos de controle, monitoração, alarme, gravação de dados e imagens relativos à segurança. Os exemplos de eventos a serem monitorados ou alarmados encontram-se descritos conforme as categorias elencadas a seguir : controle de acesso (tentativa de acesso não autorizado em portas controladas; porta aberta por tempo superior ao estabelecido; entrada de “carona”); controle de intrusão (presença de pessoas na área externa, próxima do edifício, em cinturão de segurança; tentativa de arrombamento de portas; presença de pessoas em áreas de não-

permanência); sistema antifurto (tentativa de saída com material não permitido/autorizado); proteção e alarme de incêndio (detecção de fumaça/calor em ambientes; acionamento de botoeiras do sistema; iminência de descarga de gás; abertura de válvulas de *pré-action* do sistema de *sprinklers* secos; linha interrompida ou detector removido da base; sistema bloqueado); segurança operacional de infraestrutura (ocorrência de líquidos no entrepiso; ocorrência de vapores no ambiente; campo eletromagnético elevado).²¹

A Segurança Patrimonial deve considerar diversos fatores a serem tratados, a começar pelo controle de acesso. Numa construção de alta segurança, torna-se fundamental que todo o acesso a cada uma das áreas do prédio seja controlado, monitorado e que as informações decorrentes sejam armazenadas por um período de tempo para consulta futura. Os ambientes do edifício devem ser classificados por níveis de segurança, de acordo com o grau de restrição que cada um deva ter em função de seu conteúdo. Todas as portas que dão acesso às áreas críticas devem ser controladas através de dispositivos do tipo cartões de proximidade para as áreas de baixo nível de segurança e mediante leitoras biométricas (impressão digital, palma da mão ou íris) para ambientes de alto fator de segurança. A recomendação para os controles são de que as salas de equipamentos (servidores, *mainframes*, robôs, etc.) possuam leitoras biométricas com código numérico, as salas de infra-estrutura (UPS, geradores, painéis, subestação, etc.) possuam leitoras biométricas com código numérico, as salas de operadores possuam catracas mais leitora de proximidade acoplada a teclado com código numérico e a sala de segurança possua leitora de íris.

Os requisitos mínimos do sistema de controle de acesso a ser implantado deve considerar o conjunto de fatores de maior relevância ao CPD, conforme premissas de projeto cujos detalhamentos básicos podem incluir os seguintes tópicos : duplo sentido no controle que monitore tanto a entrada quanto a saída no ambiente, com operação em rede mediante servidores exclusivos e redundantes; as portas não podem permanecer abertas e o sistema deve prever alarme para qualquer porta que assim permaneça por mais de 30 segundos; devem ser utilizadas fechaduras eletromagnéticas e prever um dispositivo “anticarona”, impedindo que 2 pessoas

ultrapassem 1 porta com um único cartão e permitindo que um indivíduo só saia de um determinado local se sua entrada tiver sido registrada; possuir um sistema autônomo de energia, com UPS ou baterias próprias, além do sistema do edifício.

O estacionamento localizado ao lado do prédio deve ter o acesso de veículos controlado por cancelas automáticas acopladas a sistema de leitura de cartão de proximidade, gerenciado pelo sistema de Gestão Predial. As vagas do estacionamento devem ser dedicadas aos funcionários do CC-*Comand Center*, NOC, SOC e *Energy Plant*, a analistas de suporte (quando alocados para mesa de crise), aos técnicos prestadores de serviços e a visitantes do CPD previamente cadastrados. Os visitantes devem ser cadastrados na recepção do prédio onde podem receber um cartão de proximidade que deve permitir o acionamento somente nas portas que dão acesso ao local a ser visitado. As tentativas de acesso indevido devem ser alarmadas imediatamente na sala de segurança. A saída de visitantes deve ocorrer mediante um dispositivo coletor de crachás, de forma a impedir que o cartão não seja devolvido.

As equipes de manutenção e operação devem possuir cartões com direito de acesso às áreas específicas de infra-estrutura, sendo que, o acesso às áreas de alta segurança deve ser estabelecido previamente, de acordo com um plano de manutenção e operação. A central de segurança deve ser prevista com uma área para operar e monitorar o sistema de acesso onde deve ficar instalado um dos servidores do sistema para o cadastramento de cartões de funcionários, com estabelecimento de horários de entrada/ saída, programação de trabalho de pessoal de operação e manutenção. O sistema de interfones deve considerar que ao lado das portas externas principais podem ser instalados os dispositivos comunicadores com os operadores da Sala de Monitoramento. O interfone mestre na sala de monitoramento deve identificar automaticamente qual o dispositivo comunicador está gerando a chamada. Qualquer acionamento dos interfones deve produzir um efeito alerta da imagem correspondente no monitor de eventos do sistema de CFTV. O interfone mestre deve ter fone e microfone tipo *hands free* (tipo operador de telemarketing). Podem ainda ser necessários alguns dispositivos complementares, de acordo com o projeto de arquitetura, nos quais devem ser previstos os dispositivos de restrição e controle de

acesso, tais como : torniquetes - dispositivos que permitem a passagem de uma única pessoa de cada vez; catracas - similar ao torniquete, porém com menor grau de segurança; catracas para deficientes - dispositivos que permitem a passagem de cadeira de rodas.

O Sistema de Alarme de Intrusão Interna e Perimetral deve ser integrado ao Sistema de Monitoração e à central de supervisão, de modo a possibilitar as prontas identificações da área violada através de plantas ilustradas na tela do computador de Supervisão. A instalação do sistema de controle e alarme perimetral deve ser operada através de um Micro Computador com *hardware* e *software* compatíveis com as necessidades dos equipamentos do sistema. O *software* de supervisão deve ser de telemonitoramento *multicasting* (multifunções ou multicanais), vinculando o setor violado com as respectivas imagens. Cada módulo perimetral de servidor deve possuir as seguintes características: 2 ou 4 portas de entradas e saídas; possibilidade para futura expansão em módulo de voz; utilizar compressão vinculando a imagem com as entradas e saídas de sinalização e comando; *software* no controlador que possibilite um pop-up^{*} da imagem vinculada ao trecho alarmado; software gráfico ilustrando o mapa dos setores perimetrais protegidos e a vinculação das imagens com cada setor.

Em todo perímetro devem ser instalados sensores de infravermelhos ativos, duplo-feixe, e devem estar conectados à rede de comunicação através de módulos servidores (módulos de captura de imagens, comandos e alarmes), os quais podem integrar imagem, voz, sinalização do setor violado, escuta de áudio perimetral e comando de voz através de amplificadores de áudio e sonofletores de potência compatível com o setor monitorado. Acessoriamente, recomenda-se a utilização de sensores de profundidade, através da utilização de cabos piezelétricos sob a grama, os quais têm sua condutividade alterada quando sujeitos a pequenas variações de pressão e indicam movimento na superfície que devem ser investigados pelo pessoal de segurança. Todos os sensores infravermelhos passivos e ativos devem ser programados via central de supervisão localizada na recepção para receber

^{*} *pop-up* – tela de aviso com abertura automática no monitor, a partir de um comando específico.

supervisão ou não. Na situação de não supervisão (INIBIDO), o ponto não deve se apresentar na tela do computador da central de segurança, já na situação de supervisão, o ponto deve se apresentar na tela piscando dando o alerta da condição de intrusão, juntamente com um sinal sonoro. Após a verificação da violação pelo operador o sinal sonoro pode ser silenciado via teclado na área violada.

A central de segurança deve ainda possibilitar o teste dos pontos via teclado, tendo ainda os seguintes módulos para facilitar a visualização de ocorrências: módulo de ilustração em planta; módulo de ilustração do estado das portas; módulo com alarme de porta-aberta vinculado simultaneamente à imagem, na própria tela da planta, do local violado; módulo de posicionamento gráfico dos componentes de segurança e da Brigada de Incêndio. Deve ser também previsto um Sistema Auxiliar de Interface de Alarme com CFTV, composto por um dos módulos do *software* de imagens que envolvem o controle múltiplo de câmeras, periféricos e alarmes, possibilitando o monitor receber imagem de câmeras associadas ao Sistema de Intrusão. Este sistema deve possibilitar o surgimento da imagem na tela gráfica que mostra a planta do local de intrusão, através de uma placa digitalizadora. Tal sistema constitui-se de um microcomputador com processador matricial de imagens e alarmes, montado para adaptar e interfacear os sensores de alarme do campo com os monitores da sala de controle, a ser integrado ao sistema de Circuito Fechado de TV que pode registrar, em tempo real, todas as imagens de todas as câmeras com alta resolução colorida. Toda vez que houver uma intrusão deve aparecer na tela gráfica do computador da sala de segurança, a planta e a imagem do local violado com a respectivo *log*^{*} no sistema, e sua gravação. Todos os pontos de intrusão e segurança devem ser tratados como pontos físicos (entrada digital) e interligados aos controladores.

O Sistema de CFTV - Sistema Digital de Circuito Fechado de TV, interligado ao Sistema de Detecção e Alarme de Intrusão Perimetral e Interna, tem como objetivo a monitoração visual das áreas internas e externas da edificação, de áreas de acesso e circulação de pessoas em geral nas áreas internas. O sistema deve estar totalmente integrado ao Sistema de Controle de Acesso e Controle de Bens. A monitoração deve

^{*} *log* – registro eletrônico no sistema por tentativa de acesso.

ser efetuada por um sistema de circuito fechado de TV com telecâmeras supervisionadas pelos operadores da console de controle. O sistema deve apresentar as seguintes características funcionais básicas : operação contínua 24 horas por dia; imagens com ausência de distorções geométricas ou linearidade; resistir a vibrações e a impactos gerados pelo dispositivo de panoramização; operação com ajuste automático aos níveis variáveis de luminosidade (diurno, noturno, luz do sol e luz artificial).

Na elaboração do projeto de CFTV devem ser observados alguns critérios que permitam maior segurança na vigilância eletrônica ao mesmo tempo em que reduzem a necessidade de operadora ou controladores para sua operação, dentre os quais, recomenda-se quanto ao posicionamento das câmeras que no interior do prédio, deve ser priorizada a cobertura dos acessos e corredores, nas salas de equipamentos, deve ser priorizada a cobertura da entrada e da saída da sala, aumentando a condição de identificação do intruso, em ambientes sem ocupação usualmente escuros, podem possuir câmeras infravermelhas ou o ambiente deve ser dotado com sensores de presença para comando de iluminação, nas áreas externas onde haja equipamentos (cobertura do prédio) ou vulnerabilidade (tomadas de ar e saída de autos), devem possuir câmeras com sensor de movimento acoplado e sua imagem deve abrir tela *pop-up* no monitor da sala de segurança sempre que ativada.

O funcionamento da console de controle deve ser baseado na matriz de comutação de vídeo, micro processada, a qual deve ser responsável por todas as funções dos sistemas e deve possuir uma configuração compatível com suas tarefas. A mesa de controle deve ser dotada de um teclado especial, o qual pode acessar o microprocessador que utiliza um programa aplicativo que deve oferecer, no mínimo, as seguintes facilidades operacionais: seleção de imagens, o que consiste na alocação de imagens de qualquer uma das telecâmeras em qualquer um dos monitores de vídeo das consoles; panoramização, o que deve ser permitido através da seleção de uma telecâmera móvel que acione o Gravador Digital de Vídeo (HDD).

A console de controle principal pode controlar a operação de gravação de modo automático, nas seguintes modalidades: gravação da imagem de uma telecâmera

qualquer através de comando de operador; operação pré-programada para um determinado horário ou evento; gravação por detecção de movimento por vídeo. As imagens gravadas podem ser duplicadas para arquivamento em mídia externa, de forma a utilizar o *hardware* de gravação de forma contínua, sobrescrevendo imagens às anteriores. Para que se mantenha no *hardware* um arquivo de imagens de no mínimo 1 mês, sua capacidade de gravação deve ser dimensionada de acordo com a previsão de tempo diário de gravação de imagens. O Sistema de TV deve apresentar características operacionais que atendam aos requisitos funcionais mínimos de segurança da Edificação. Cada seqüenciamento por área deve ser feito através de programação preestabelecida pelas consoles. Através deste processo, o operador pode monitorar visualmente várias áreas supervisionadas. Cada sequenciamento pode ser apresentado em um monitor, onde cada imagem deve ser apresentada por um período de tempo suficiente para a detecção de irregularidades por parte do operador.

Após serem selecionadas pelo operador, todas telecâmeras, que devem possuir acionadores de rotação vertical, horizontal e de movimentação da lente, podem ser comandadas remotamente pelo mesmo. O objetivo desta operação é o acompanhamento por parte do operador de qualquer movimentação e/ou detalhe que estejam ao alcance da telecâmera. Após sua utilização, a telecâmera móvel deve retornar a uma posição de repouso preestabelecida, tendo nesta posição a visão de uma telecâmera adjacente. Todas as telecâmeras devem estar cobertas por pelo menos uma adjacente. Nas áreas de cobertura crítica (proteção perimetral e salas de arquivos de mídia), podem ser adotadas as câmeras de controle automático conjugadas aos sensores de cobertura de movimento, de forma a automaticamente direcionar as mesmas à área de onde surgiu o alarme, facilitando ao operador a confirmação de intrusão. Na instalação, deve ser observada a compatibilidade entre câmeras e lentes com a intensidade de iluminação do ambiente supervisionado. Devem ser previstas estruturas de suporte e proteção das câmeras adequadas para a montagem em áreas internas e externas. O CFTV deve possuir uma central de controle e gravação microprocessada para gravação digital das imagens geradas pelas câmeras. Esta central deve ter função de multiplexador de modo a possibilitar a divisão da tela do monitor em telas menores, cada uma responsável pela visualização

em tempo real de uma câmera, e gravar simultaneamente todas as imagens geradas pelas câmeras a elas associadas. Através deste equipamento deve ser possível escolher qual câmera pode ser apresentada em cada sub-tela e de controlar automaticamente as câmeras. O CFTV deve permitir o acesso das imagens de qualquer câmera na rede local do prédio, por meio de *software* específico. As imagens de todas as câmeras devem ser observadas em tempo real, em modo multiplexado, devendo ter capacidade adequada para armazenar as imagens em HDD. O CFTV deve também possibilitar a gravação remota em diversos tipos de equipamentos que tem por função a gravação constante das imagens vindas do gravado digital.³⁶

Podem ainda serem consideradas outras características que devem ser preenchidas pelo sistema como descrito em análises que seguem. O sistema de CFTV pode ser integrado ao sistema de gerenciamento de segurança, sendo fornecida resposta a eventos do controle de acesso e sistemas de alarme, de modo a permitir a designação da imagem de uma câmera específica para um monitor específico, diante da ocorrência de uma condição ou evento de alarme pré-definido. O sistema de CFTV deve adotar câmeras infravermelhas para ambientes externos de baixa luminosidade e para salas escuras. O sistema de CFTV pode permitir o seqüenciamento de câmeras selecionadas, a diferentes intervalos de tempo, a serem exibidas em um monitor selecionado. O sistema de CFTV deve ser totalmente sincronizado, de modo a assegurar que não haja faixas verticais nos monitores. As câmeras selecionadas devem ser gravadas continuamente, 24 horas por dia, além dessas câmeras, qualquer imagem de um evento de alarme deve ser gravada também, com tomadas preferenciais. O sistema de CFTV deve permitir a programação de legendas para imagens de quaisquer câmeras exibidas nos monitores que façam parte da seqüência automática ou tenham sido selecionadas manualmente, incluindo-se a localização, dia, horário e *status* do alarme.

O Controle de Bens por Sistemas Antifurto deve considerar os ativos como *laptops*, projetores e outros que devem ser protegidos através de *labels* (etiquetas de elevada resistência) a serem instalados no interior ou fixados na parte externa destes

equipamentos. As antenas colocadas nas saídas devem detectar a presença destes *labels* a fim de evitar o furto ou desvio destes materiais. Nas saídas onde houver controle de acesso (catracas ou portas), o sistema de controle de ativos deve integrar-se ao de controle de acesso com as seguintes respostas: saída de ativo não associado a nenhum crachá ou ao crachá errado – alarme sonoro e travamento da catraca ou porta; saída de ativo vinculado a um crachá específico - liberação da catraca após leitura do crachá pela leitora.

O sistema antiarrombamento, de detectores de vapores explosivos e proteção contra intrusão nas tomadas de ar do sistema de ar condicionado deve considerar a previsão de sensores de vibração (sensores sísmicos) nos principais pontos de intrusão por arrombamento, interligados aos módulos de captura de imagem e alarme de modo a ilustrar no ambiente gráfico os locais de violação, realizando o *pop-up* das imagens no instante da violação da área. Nos principais acessos ao CPD devem ser instalados os detectores de vapores explosivos integrados ao sistema de CFTV e controle de acesso. Nas tomadas de ar do sistema de ar condicionado devem ser instalados sensores de presença conjugados com sensores de microondas de modo a detectar intrusão, sendo recomendável que nestas tomadas de ar sejam instaladas proteção mecânica antiintrusão, bem como câmeras para integração do sistema de intrusão com o sistema de CFTV.

A instalação de sistemas de Proteção e Alarme de Incêndio tem a função de proteger a vida dos ocupantes, o conteúdo da instalação e a integridade da construção, nesta ordem. Para isto, numa instalação de alta disponibilidade diversos tipos de sistemas disponíveis devem ser considerados, atuando de forma escalonada, obedecendo a seguinte sequência de atuação: detectar princípio de incêndio, através da análise por amostragem do ar ambiente identificando na composição do ar gases ou substâncias que indiquem a ocorrência de aquecimento anormal nas instalações; detectar presença de fumaça, chama ou elevação anormal de temperatura ambiente; combater um princípio de incêndio manualmente, com extintores autônomos, e automaticamente, por meio de sistemas de inundação de gás; combater um incêndio através da inundação de gás automaticamente; combater um incêndio que não foi contido nas formas anteriores através de dispersão de água (chuveiros).

Os critérios gerais devem considerar que o projeto arquitetônico possa ser elaborado tendo em vista a preocupação com a ocorrência de incêndios, assim, devem ser analisados aspectos como: utilização de materiais incombustíveis ou auto-extinguíveis; segmentação entre ambientes, separados de forma a não permitir a propagação de fogo de uma área para outra, facilitando o combate setorizado; interface entre sistemas prediais, que automaticamente executem tarefas como o desligamento de sistemas de ar condicionado em caso de alarme de incêndio, o destravamento de portas em caso de sinistro, facilitando a evacuação do local e o fechamento de *dumpers* automáticos.²¹

Nas áreas de maior risco operacional (salas de computadores e *mainframes*, equipamentos de telecomunicações, baixa plataforma) deve ser utilizado um sistema de detecção precoce de incêndio. Este sistema, também conhecido como sistema de detecção por amostragem de ar, consiste em uma rede de tubos que levam o ar coletado nas áreas de proteção para uma central de análise do ar, utilizando um sistema de exaustão. Na central, o ar é analisado por espectro, através de raio laser, identificando a presença de gases oriundos de um princípio de combustão. Normalmente os alarmes possuem de 3 a 5 níveis de criticidade, identificando desde um risco remoto até um princípio de incêndio. Os níveis de criticidade podem ser ajustáveis via *software*, com base em faixa-padrão de número de partículas discretas de determinado tamanho, como produto de combustão, por um tempo específico de amostragem. Os níveis de alarme podem ser estabelecidos como segue: Estado Normal; Falha na Central; Pré-alarme nível 1 no caso de ocorrência de partículas na faixa inferior (baixo risco); Pré-alarme nível 2 no caso de ocorrência de partículas na faixa intermediária (baixo risco); Alarme nível 1 no caso de ocorrência elevada de partículas na faixa média (risco); Alarme nível 2 no caso de ocorrência elevada de partículas na faixa superior (alto risco).

A Central de Detecção deve ser configurada via *software* que deve permitir monitorar, configurar e ler histórico do detector. As características do *software* de processamento de sinais avançados do detector devem permitir ainda que a resposta

do detector seja moldada ao ambiente em que ele está instalado. Isto proporcionará uma detecção mais sensível com um mínimo de alarmes não desejados. São recomendáveis no mínimo os seguintes ajustes para alarme: 2 pré-alarmes e 2 Níveis de Alarme – programáveis em incrementos de 5% da saída selecionada do detector. Alarme Nível 2 e Pré-alarme Nível 2 são opcionais; Alarmes Dia/ Noite – um segundo jogo de níveis de alarme programados devem estar disponíveis durante o período noturno que permite que a resposta do detector seja mais sensível durante o dia; Atrasos do Alarme – programável de 0 a 60 segundos para cada nível de alarme. Os atrasos podem ser usados para eliminar alarmes não desejados causados por condições transientes; Trinco do alarme – uma opção que permite condições de alarme permanecerem ativas até o reset, ou resetar automaticamente depois de um atraso programável de 0 a 60 minutos; Média do Sinal de Fumaça – Uma opção que calcula a média o nível de fumaça em um período programável de 2, 4, ou 8 segundos. Isto pode ser usado para eliminar picos no nível de fumaça causados através de fumaça passageira. O sistema deve ser instalado no ambiente e no entrepiso, e sua central deve ser interligada à central de detecção pontual, para, em conjunto, operar os sistemas de combate automático a incêndio.

O Sistema de Detecção de Incêndio Pontual constitui-se daquele tipo recomendado para detecção de incêndios que inclui detectores óticos e iônicos de fumaça, instalados no ambiente, entrepiso e entreferro das áreas críticas, detectores de chama para áreas classificadas e detectores de calor e incremento de calor no tempo (termo – velocimétricos) para escritórios e áreas de utilidades. Os detectores devem ser providos de ajuste automático de sensibilidade, e o cálculo de área de cobertura deve levar em conta o número de trocas de ar por hora em cada ambiente. O sistema utilizado deve ser digital endereçável via *software*, e a seqüência típica de operação deve ser como descrito a seguir : na detecção de um único elemento, a central deve soar um alarme intermitente. Este elemento pode ser um detector, um acionador manual ou mesmo um sistema de detecção precoce; na detecção de um segundo elemento no mesmo ambiente, o tom do alarme deve ser alterado para som contínuo, ao mesmo tempo em que Dumpers automáticos são fechados, os sistemas de ar condicionado e ventilação do ambiente são desligados, as fechaduras

eletromagnéticas são liberadas e é iniciada a contagem de tempo para liberação de gás e abertura das válvulas de *pré-action* do sistema de chuveiros de água a seco (dry-sprinklers); a liberação de gás no ambiente e a abertura da válvula de *pré-action* devem ser precedidas pelo desligamento de toda energia elétrica do ambiente protegido.

Visando impedir o desligamento dos equipamentos devido a um princípio de incêndio que pode ser controlado manualmente, ou mesmo em caso de um alarme falso, devem ser considerados 2 (dois) dispositivos: temporização regulável do retardo de disparo do gás; uma chave de bloqueio de descarga do gás, instalada no interior do ambiente protegido. Ainda pode ser recomendável que o sistema de detecção permita uma interface com o sistema de Inteligência Predial e que sejam criadas telas de supervisão que mostrem a planta do prédio, sendo que, na ocorrência de um alarme, o dispositivo atuado seja mostrado na planta do pavimento, permitindo a rápida visualização e constatação do evento alarmado. Os detectores instalados no entrepiso e entreforro devem ter indicação no forro do ambiente, através de setas para baixo (entrepiso) ou para cima (entreforro), facilitando também a constatação do estado do dispositivo.

Os Sistemas de extinção de incêndio devem considerar que, em ambientes de alta tecnologia com presença maciça de equipamentos de processamento de dados, há uma necessidade premente de proteção dos dados, minimização de danos dos equipamentos e um rápido restabelecimento das condições operacionais, em caso de ocorrência de um princípio de incêndio. Assim, visando garantir uma melhor proteção aos equipamentos e reduzir danos aos ativos de alto valor, pode ser aconselhável a instalação de sistemas conjugados de combate automático por inundação de gás e por chuveiros de água com tubulação seca. A conjugação entre estes 2 (dois) sistemas pode permitir a identificação de uma condição de incêndio e liberação do gás extintor previamente à liberação de água para a tubulação de *sprinklers*. Isto visa dar tempo ao pessoal de operação para verificar a extinção do fogo e evitar os danos decorrentes da utilização de água nos equipamentos.

O Sistema de combate por inundação de gás no ambiente são extremamente eficientes quando comparados a sistemas de *sprinklers*, sobretudo em ambientes onde o fogo pode iniciar-se dentro de equipamentos em racks, onde a água não atinge facilmente. Já um sistema a gás ocupa em pouco tempo todo o ambiente protegido, extinguindo um incêndio em poucos segundos, impedindo-o de alastrar-se para equipamentos vizinhos. Além disso, o combate pode ser feito sem a desenergização dos equipamentos, minimizando tempos de parada. Os gases disponíveis para este tipo de aplicação são os Inergen e o FM – 200, e os projetos com cada um deles são bastante diferentes. Algumas características podem ser citadas como segue : Inergen – constitui-se de um sistema de alta pressão, e requer uma quantidade grande de cilindros para proteger um ambiente; os cilindros podem ser instalados a grande distância da área protegida, permitindo uma Central de Cilindros de gás; Permite o uso de válvulas direcionais; assim, uma única bateria de cilindros pode efetuar o combate em vários ambientes distintos, embora neste caso seja necessária uma bateria de cilindros reserva; É um gás de baixo custo, em caso de necessidade de reposição do mesmo; O dimensionamento de tubulações é mais flexível, permitindo pequenas alterações de layout sem necessidade de alteração do sistema; Por ser de alta pressão, requer a utilização de *Dumpers* de alívio nos ambientes, previamente acionados em casos de inundação; FM 200 - constitui-se de um sistema de baixa pressão, onde os cilindros devem ficar próximos ou no interior do ambiente protegido; Dificilmente podem ser usadas válvulas direcionais, devido à baixa pressão do propelente; O número de cilindros é bastante reduzido; O custo de reposição é alto, pois se trata de gás importado; O dimensionamento do sistema é inflexível, e qualquer alteração na dimensão dos ambientes ou mesmo em comprimentos de tubulação requer uma revisão geral do cálculo hidráulico.²¹

As características típicas do sistema de combate, independente do tipo de agente adotado, onde há um conjunto de dispositivos de combate por inundação pelo agente extintor, pode ser composto pelas seguintes partes: Um cilindro ou conjunto de cilindros com o agente extintor, dimensionados e carregados para uma área específica; um tubo coletor, no caso de 2 ou mais cilindros para um único ambiente; Uma rede de tubulações apropriadas, calculadas hidraulicamente, para levar o gás até

os difusores; Um conjunto de difusores de gás, instalados no ambiente e entreposto da área protegida; cabeças de disparo elétricas no cilindro principal e comutadores a pressão nos demais cilindros de um único ambiente, garantindo simultaneidade na liberação do gás; Acionadores manuais de liberação do gás nos cilindros principais, permitindo a liberação do agente mesmo em caso de falha nos sistemas de detecção, ou atuação automática; Chaves de bloqueio de gás, permitindo abortar momentaneamente o disparo do gás.

O combate por chuveiros secos (*Dry Sprinklers*), cuja adoção para o combate a incêndio em edifícios é uma norma tanto local (ABNT, Corpo de Bombeiros) quanto internacional (NFPA, FM), contudo, quando se trata de edifícios ou ambientes ocupados por equipamentos de Processamento de Dados, cujo valor (entre equipamentos e informações) é extremamente elevado e cujas consequências, num caso de utilização de água para combater um incêndio ou sobretudo no caso do rompimento acidental de um bulbo, são extremamente danosas, o conceito de chuveiros convencionais deve ser revisto. A NFPA 75 recomenda que um sistema de chuveiros automático para proteção de áreas de computadores seja separado do sistema do restante da edificação, e isolado por meio de válvulas eletromecânicas. Assim, a obediência à norma pode ser obtida através do uso de um sistema de chuveiros secos (*Dry Sprinklers*). Neste sistema, uma válvula eletro-mecânica é instalada no ramal que atende à área protegida, e permanece fechada. Sua atuação é independente do rompimento dos bulbos dos chuveiros, e é feita pelo sistema de detecção de incêndio, na ocorrência de uma detecção que venha disparar o gás do sistema de combate, liberando água na tubulação e disponibilizando a mesma, caso o gás não controle o incêndio e qualquer dos bulbos venha a romper-se. Na condição de repouso, a tubulação dos chuveiros é pressurizada pneumaticamente, e uma queda na pressão interna do sistema é imediatamente alarmada na Central. Assim, tanto o rompimento de um bulbo acidentalmente quanto um vazamento na tubulação devem ser detectados de pronto, sem o risco de descargas de água no ambiente. O sistema deve ser dotado, ainda, de um dreno no ponto mais baixo para que, após uma abertura da válvula, toda a água possa ser retirada da tubulação e a mesma pressurizada novamente.

Os sistemas acessórios que visam melhorar a eficiência da atuação dos sistemas de proteção e alarme de incêndio, bem como garantir que um incêndio fique restrito à área de origem, podem compor o projeto que deve prever os dispositivos do tipo: dumpers corta-fogo automático, comandado pelo sistema de detecção, que se fecham antes do início de combate automático, sendo que, isto garante a concentração de gás desejada no ambiente e evita propagação para áreas contínuas; Paredes e portas classificadas como F – 90 entre as áreas; Sistema autônomo e ininterrupto para prover inércia para a central e dispositivos de acionamento; Sistema de fechamento de todas as aberturas do ambiente para as demais áreas (passagem de cabos, eletroduto, bandejas e leitos) com materiais apropriados, do tipo *Fire Blocks* (bloqueadores de fogo) garantindo a estanqueidade ambiente e a não propagação de incêndio.

Além disso, as áreas de utilidades também devem ser adequadamente protegidas, pois um incêndio numa delas terá quase o mesmo efeito que um nas salas de computadores, pois poderá privar os mesmos do suprimento de energia. Nas áreas de utilidades, a recomendação pode ser pela utilização dos seguintes sistemas: Salas de painéis elétricos, UPS's subestações - Detecção pontual, com detectores de calor e fumaça e Combate por inundação de gás; Salas de baterias - se isoladas e com elementos abertos, Detecção de Hidrogênio e Combate por água; Salas de geradores - Detecção pontual, com detectores de fumaça, de calor e de chama, sendo o Combate por inundação de gás (deve ser analisado, neste caso, o uso do CO₂) ou sistema de dilúvio.

A Segurança Operacional de Infra-estrutura, como complemento às instalações de Segurança Patrimonial e contra incêndio, devem ser previstas em instalações que, através de alarmes ou ações, aumentem ainda mais os níveis de qualidade das operações por detectar certos riscos antes que os mesmos causem danos à integridade das pessoas, dos equipamentos e das informações que são processadas no ambiente. Entre os sistemas acessórios e sua utilidade, devem ser destacados os seguintes: Detecção de líquidos e vapores - a utilização de piso elevado em CPD's traz grandes

facilidades para a distribuição elétrica, lógica e de ar condicionado, contudo, principalmente após o advento das unidades condicionadoras de ar de precisão que podem ser instaladas no próprio ambiente dos computadores, há um aumento do risco da presença de água no entrepiso, como decorrência de fatores tais como entupimento de drenos de condensado, ruptura na tubulação de água que alimenta os sistemas de umidificação, dentre outros. Dependendo da quantidade, a água pode causar curto – circuito nas instalações elétricas e provocar incêndios ou atuação de protetores. Como o entrepiso não é uma área monitorada visualmente, deve ser previsto um sistema de detecção de líquidos interligado ao sistema de supervisão de utilidades; Interferências Eletromagnéticas - não obstante a construção deve prever que os ambientes possam se comportar como “Gaiolas de Faraday”, com uma proteção eficaz contra campos magnéticos externos que também podem ocorrer no interior do edifício e sua presença é uma ameaça ao funcionamento correto de equipamentos eletrônicos e de comunicação. Assim, ambientes de equipamentos devem possuir malha referencial de terra contra interferências de alta frequência, conectadas adequadamente a *taps* equipotenciais devidamente aterrados. Detectores de campos magnéticos também poderão ser previstos nas áreas críticas; Botões de desligamento - Meios e condutores elétricos são à base da infra-estrutura de um CPD, pois levam energia condicionada dos equipamentos vitais para o funcionamento da instalação. Por outro lado, são fontes de risco de incêndio, uma vez que fugas a terras, curto-circuito ou mesmo sobrecorrentes podem gerar aquecimento nos cabos e vir a provocar chama. É usual a utilização de botões de emergência (também chamados de *panic buttons*) em ambientes de equipamentos. Estes botões, uma vez acionados, desligam toda a energia elétrica de uma sala, um setor ou mesmo todo um andar de uma instalação, evitando um incêndio que um circuito elétrico venha danificar outros condutores, que passaria a se tornar novos focos potenciais de um incêndio, em um efeito dominó. Por outro lado, o acionamento indevido de um botão destes ocasionará uma paralisação de um grande número de equipamentos sem necessidade, gerando grandes perdas em informação e mesmo em imagem do cliente. Assim, a utilização deste tipo de dispositivo deve ser, exaustivamente discutida e, se adotadas, devem obedecer às recomendações que seguem. A botoeira de desligamento deve ser instalada junto à saída do ambiente, e

ser adequadamente sinalizada quanto à sua função e decorrências. Deve ser à prova de acidentes (botão protegido contra acionamento por descuido), com caixa protetora de acrílico. Deve ser setorizado, desligando unicamente a áreas onde o mesmo encontra-se instalado. Deve ser do tipo “estado natural de repouso” ou contato aberto, impedindo que uma interrupção de fração venha a acionar o desligamento.

Quanto às edificações ou estruturas, as condições mínimas constantes das normas ABNT devem ser compatíveis com o nível de proteção adequado à determinada estrutura, com base nos seguintes fatores: geometria da estrutura, modo de utilização da mesma, frequência esperada quanto à incidência de descargas atmosféricas, e considerações sobre os efeitos e as conseqüências das descargas atmosféricas nas estruturas, e os perigos causados ao seu conteúdo e aos arredores das mesmas as estruturas são classificadas em estruturas comuns ou especiais. Como efeitos diretos perigosos, podem ser citados: fogo, dano mecânico à estrutura, ferimentos a pessoas e/ou animais, danos em equipamentos elétricos e eletrônicos.

Os efeitos das descargas atmosféricas podem também ser responsáveis por pânico, causar explosões, emissões de substâncias perigosas tais como materiais radioativos, agentes químicos, substâncias bioquímicas contaminadoras, bactérias, vírus, dentre outros. Cabe observar que os efeitos indiretos das descargas atmosféricas podem particularmente causar danos (interferências, incluindo-se à queima) em equipamentos eletrônicos sensíveis de uma maneira geral. A atenuação/ eliminação destas interferências deve ser prevista quando da especificação da proteção interna. As estruturas, de uma maneira geral, são classificadas em estruturas comuns (de utilização ordinária com propósitos comerciais, industriais, agrícolas, administrativas e residenciais) e estruturas especiais (aquelas cujo tipo de ocupação implica em riscos confinados ou para arredores ou para o meio ambiente, ou para as quais o SPDA requer critérios de proteção específicos), sendo esta última sub-classificada, basicamente em quatro tipos - estruturas especiais com risco de confinamento (cujos materiais de construção, conteúdo ou tipo de ocupação tornam todo o volume da estrutura vulnerável aos efeitos perigosos de uma descarga atmosférica, porém, com estes danos restringindo-se ao volume da própria estrutura, por exemplo: estação de telecomunicações, usinas elétricas, indústria com áreas classificadas etc); estruturas

especiais com risco aos arredores (cujo conteúdo pode ser perigoso para os arredores, quando atingidas por uma descarga atmosférica, tais como depósito de explosivos ou líquidos de inflamáveis, no caso do CPD, este item se aplica ao tanque de combustível do sistema de geração e energia de emergência); estruturas especiais com risco ao meio ambiente (aquelas que quando atingidas por uma descarga atmosférica podem produzir emissões biológicas, químicas ou radioativas, como por exemplo: indústrias químicas, usinas nucleares, fábricas ou depósitos de produtos tóxicos, sendo que, este item não se aplica aos ambientes de CPD); estruturas especiais diversas (onde o SPDA requer a utilização de critérios específicos de proteção, estruturas tais como - Chaminés de grande porte; Estruturas contendo líquidos ou gases inflamáveis; Antenas externas de televisão; Estruturas em construção; Barracas, locais de camping, campos de esporte; Instalações temporárias; Barcos).

A Iluminação de Emergência deve ser mantida em todos acessos (rotas de fuga) e saídas, sendo que em no máximo 10 segundos o sistema de iluminação de emergência deve atender as rotas de fuga e saídas, nos casos de queda da energia comercial ou emergencial, operando com total confiabilidade por um tempo mínimo de 90 (noventa) minutos. Os sistemas de iluminação de emergência alimentados por baterias são mais confiáveis e econômicos que os alimentados por geradores, sendo o mais apropriado para utilização em ambientes de Missão Crítica. Se faz recomendado que 10% da iluminação total do ambiente de equipamentos de Missão Crítica seja destinado para iluminação de emergência nas rotas de fuga e saídas e em áreas muito extensas, salas de equipamento de “*Facilities*” (UPS, Geradores, Ar-condicionado, dentre outros) se faz recomendado que 25% da iluminação total necessária para o local, seja destinado para o sistema de iluminação de emergência. Nas rotas de fuga devem ser utilizadas luminárias de aclaramento (do tipo fluorescente) com nível de iluminação de 150 (cento e cinquenta) Lux. Nas saídas devem ser utilizadas luminárias de balizamento (do tipo incandescente), com nível de iluminação de 50 (cinquenta) Lux. Ambas luminárias (aclaramento e balizamento) devem ser de modelo autônomo alimentadas por bateria e com autonomia mínima de 90 (noventa) minutos.

4.5 Cabeamento Lógico

O Cabeamento Lógico ou Cabeamento Estruturado deve prover o compartilhamento de informações e de recursos de informática e telefonia, atendendo todos os servidores e equipamentos distribuídos nas salas do CPD, conforme layout definido no projeto executivo. A rede deve ser preparada para trafegar vários tipos de aplicações, tais como *Ethernet/Fast-Ethernet/ Gigabit Ethernet/ATM*. Devem ser utilizados cabos UTP 4 pares categoria 6 (obs: cat 6 ou variantes diferenciadas quando for o caso – cat 5e ou cat 6a), visando atender o layout dos equipamentos dentro das salas do CPD. Para terminação dos cabos UTP 4 pares oriundos dos *switchs* devem ser instalados no rack os *patch panels* modulares para até 24 portas. Quando necessário, devem ser utilizadas as conexões em fibra óptica e *patch panels* ópticos. Para atendimento ao sistema de voz devem ser instalados no rack os *patch panels* de 24 portas para conectorização do cabo proveniente do DG-Distribuidor Geral. Os cabos devem ser acomodados em leitos aramados do piso técnico. Para assegurar a proteção e preservação da integridade dos cabos destinados a Cabeamento Estruturado, a infra-estrutura deve estar em total conformidade com todos os requisitos estabelecidos pelas normas técnicas aplicáveis neste seguimento, sendo os mesmos diretamente relacionados à performance e disponibilidade da transmissão de sinais de dados. Após a conclusão dos serviços devem ser executados testes de certificação utilizando os mais modernos equipamentos de testes (Nível III, como por exemplo, o Fluke DSP-4000). Estes equipamentos devem estar preparados para testar o cabeamento instalado em todos os requisitos de performance estabelecidos pela EIA/TIA para Categoria 6, tais como *NEXT, Attenuation, FEXT, Return Loss, ELFEXT, PSNEXT, PSFEXT, PSELFEXT, Delay Skew, Propagation Delay, ACR, PSACR*.^{*} Todos os serviços devem ser executados rigorosamente segundo recomendações das normas técnicas vigentes (Exemplos : ANSI/EIA/TIA-568 A, ANSI/EIA/TIA-569 A, ANSI/EIA/TIA-606, ANSI/EIA/TIA-607, TSB 67, TSB72, TSB95 e, até mesmo, quando publicada a ANSI/EIA/TIA-942) para

^{*} Tipos de testes recomendados para os cabeamentos lógicos pelas normas ANSI/EIA/TIA.

O sistema de Monitoração e Inteligência Predial deve ser capaz de integrar múltiplas funções dos subsistemas, incluindo supervisão e controle, gerenciamento de alarmes, coleta e armazenamento de dados históricos, sendo imprescindível ao controle de Infra-estrutura Física na Operação e Manutenção do CPD. Tal sistema deve ser instalado em máquinas redundantes e, portanto, em conformidade com todo o projeto de infra-estrutura, no mínimo N+1, o qual deve estar localizado na sala de Operação e Manutenção da Gestão de *Facilities* do CPD. Algumas telas deste sistema devem ser disponibilizadas na Cabine de Comando do CPD para visualizações, principalmente em situações de emergência ou de crises. Todos os dados devem ser disponibilizados em telas gráficas, de fácil visualização e manipulação, o que se convencionou chamar de *user-friendly* simplificação de leitura ao operador. A partir de uma tela geral que compreende toda a instalação do CPD, o operador pode acessar os subsistemas que integram as instalações físicas, tendo acesso a dados funcionais para o gerenciamento e monitoramento. A indicação do *status* de funcionamento dos equipamentos que compõem os subsistemas deve ser representada através de esquemas gráficos, representando funcionamento normal, funcionamento em emergência, defeitos e demais *status* possíveis.

No caso de mudança de status ou ocorrência de alarmes em qualquer subsistema da infra-estrutura física, o sistema de Monitoração e Inteligência Predial deve informar imediatamente ao operador, através de sinal sonoro e abertura de tela de alarme do respectivo subsistema, visando que sejam verificadas a situação e tomada as devidas providências. Todos os parâmetros elétricos e mecânicos mensuráveis dos subsistemas de infra-estrutura devem ser monitorados, em tempo real, possibilitando emissão de gráficos e relatórios que permitam análise do comportamento das instalações, bem como detectar possíveis anomalias, sendo fundamental que o sistema tenha capacidade de armazenar dados históricos para comprovação, seja por qualidade ou pela necessidade de análises regressivas do funcionamento dos equipamentos, contando com os backup's de dados de periodicidades anual, mensal, semanal e diários. Assim sendo, todos os equipamentos microprocessados que integram os subsistemas de infra-estrutura física devem possuir interface de comunicação de dados, com protocolo aberto, para que o sistema de Monitoração e

Inteligência Predial possa integrar e gerenciar todos os subsistemas prediais. Os equipamentos com protocolos fechados devem ser evitados em todos os subsistemas das instalações necessárias para o funcionamento do CPD.

Na entrada de energia devem ser monitoradas todas as linhas de energia que alimentam o CPD, através da medição dos níveis de tensão e corrente, a partir de interface com os multimedidores instalados nos cubículos de entrada, sendo os seguintes parâmetros desejados – corrente (supervisão dos valores eficazes de corrente nas três fases, em tempo real, alarmando em caso de sobre-corrente e/ou desbalanceamento entre as fases); tensão (supervisão dos valores eficazes das tensões entre fases, alarmando em caso de sub ou sobre-tensões); potência (medição das potências aparente ativa e reativa; fator de potência, consumo e demanda). Deve ser inclusa também a monitoração de status de disjuntores e seccionadoras de linha, os alarmes de atuação de relés de proteção dos circuitos, com indicação do tipo de proteção atuada, bem como, a monitoração em tempo real da temperatura dos enrolamentos dos transformadores, sinais de pré-alarme e alarme de sobre-temperatura, além do acionamento automático de sistemas de correção de fator de potência.

No sistema Emergencial de Suprimento de Energia (Grupos Moto-Geradores Diesel) devem ser monitorados os controladores do sistema de comando e controle do sistema emergencial de suprimento de energia mediante *interface* com o sistema de Monitoração e Inteligência Predial visando o gerenciamento dos seguintes parâmetros desejados - medição dos valores de tensões e frequência da entrada de rede da Concessionária, alarmando falta de fase, sub e sobre-tensões; medição dos valores de tensões e frequência da entrada de rede emergencial, alarmando sub e sobre-tensões e sub e sobre-frequência; medição dos valores de correntes por fases, potência aparente, ativa e reativa e fator de potência da saída de carga dos quadros de transferência automática (QTA's). Além dos parâmetros elétricos, devem também ser monitorados os seguintes parâmetros: *status* de rede presente (Concessionária ou Emergencial); supervisão de *status* de chaves/ disjuntores do QTA's; *status* de alarmes para a pressão de óleo, sub ou sobre-velocidade, sub ou sobre-frequência,

sub ou sobre-temperatura, falha de partida do gerador, falha de bateria, etc; monitoramento do volume de combustível dentro dos tanques de óleo diesel, alarmando quando estes níveis se tornam críticos, bem como acionando os sistemas de reposição automática aos tanques diários.

Nos Quadros Gerais de Baixa Tensão (QGBT's) e Quadros Gerais de Energia Crítica (QGEC's) devem ser monitorados os parâmetros da entrada de energia que alimenta os painéis elétricos, através da medição dos níveis de tensão e corrente, a partir de interface com os multimedidores instalados nos painéis, sendo os seguintes parâmetros desejados – corrente (supervisão dos valores eficazes de corrente nas três fases, em tempo real, alarmando em caso de sobre-corrente e/ou desbalanceamento entre as fases); tensão (supervisão dos valores eficazes das tensões entre fases, alarmando em caso de sub ou sobre-tensões); potência (medição das potências aparente, ativa e reativa); fator de potência, consumo de KWh/KVAr e demanda; níveis de harmônicos de tensão e corrente presente. Além dos parâmetros elétricos, devem ser também monitorados os seguintes parâmetros: supervisão de status de disjuntores de entrada e principais disjuntores de saída; alarme de atuação de relés de proteção dos circuitos, com indicação do tipo de proteção atuada; alarme de atuação do sistema de proteção contra surtos elétricos.

Nos sistemas de energia ininterrupta (UPS's) e Quadros de By-Pass Externo devem ser monitorados os parâmetros disponíveis nos painéis gráficos dos UPS's, sendo desejado no mínimo, as seguintes informações: medição dos valores de tensões e correntes por fases, potência aparente, ativa e fator de potência, da entrada dos UPS's; medição dos valores de tensões e correntes por fases, potência aparente, ativa e fator de potência, da saída dos UPS's; tensão e corrente (descarga, recarga e flutuação) das baterias; alarmes individuais; resumo de defeitos e falhas; *status* de funcionamento de componentes (retificador, inversor, *by-pass* interno, quadro de *by-pass* externo, baterias e disjuntores), preferencialmente através de tela gráfica.

Nas Chaves Estáticas de Transferência (STS's) devem ser monitorados os parâmetros disponíveis nos painéis gráficos, sendo desejado no mínimo, as seguintes informações: medição dos valores de tensões e correntes por fases e frequências da

entrada da fonte preferencial de alimentação; medição dos valores de tensões e correntes por fases e frequências da entrada da fonte alternativa de alimentação; potência ativa e aparente de saída; níveis de harmônicos; correntes de fuga a terra; históricos de alarmes; históricos de transferências entre as fontes; resumo de defeitos e falhas; *status* de funcionamento de componentes internos (chaves estáticas, disjuntores principais e disjuntores de *by-pass*), preferencialmente através de tela gráfica.

Nos Painéis de Distribuição de Energia de Precisão (PDU's) deve ser monitorada a entrada de energia que alimenta os painéis elétricos, através da medição dos níveis de tensão e corrente, a partir de interface com os multimedidores instalados nestes, sendo os seguintes parâmetros desejados – corrente (supervisão dos valores eficazes de corrente nas três fases, em tempo real, alarmando em caso de sobre-corrente e/ou desbalanceamento entre as fases); tensão (supervisão dos valores eficazes das tensões entre fases, alarmando em caso de sub ou sobre-tensões); potência (medição das potências aparente, ativa e reativa); fator de potência, consumo e demanda; distorção harmônica total; corrente de fuga a terra. Além dos parâmetros elétricos devem ser também monitorados os seguintes parâmetros: supervisão de *status* de disjuntores de entrada e principais disjuntores de saída; alarme de atuação de relés de proteção dos circuitos, com indicação do tipo de proteção atuada; monitoração em tempo real da temperatura dos enrolamentos dos transformadores, sinais de pré-alarme e alarmes de sobre-temperatura.

No sistema de Energia Auxiliar (Retificador 48 VDC) devem ser monitorados os parâmetros de operação, sendo desejado no mínimo, as seguintes informações: medição dos valores de tensões e correntes por fases, potência aparente, ativa e fator de potência, da entrada do retificador; tensão e corrente (descarga, recarga e flutuação) das baterias; medição dos valores de tensão, corrente e potência consumida pela carga; alarmes individuais dos módulos retificadores; resumo de defeitos e falhas; *status* de funcionamento de componentes (retificadores, bancos de baterias e disjuntores), preferencialmente através de tela gráfica.

O sistema de Controle de Acesso e Intrusão também deve ser monitorado via a integração ao sistema de Monitoração e Inteligência Predial, isto significa um nível a mais de redundância no sistema de controle de Acesso e Intrusão já que o mesmo deve estar centralizado na Sala de Segurança, deste modo, todo e qualquer alarme, seja ele a partir dos acessos internos do prédio do CPD ou a partir dos sensores perimetrais de proteção da área onde se encontra o prédio do CPD, deve ser imediatamente transferido ao sistema de Monitoração e Inteligência Predial para que o operador possa visualizar o ocorrido. O sistema deve possuir interface de comunicação com o sistema de Monitoração e Inteligência Predial, de tal modo que todas as áreas abrangidas pelo sistema de controle de acesso e intrusão sejam representadas em telas gráficas indicando o posicionamento das portas de acesso controlado e sensores perimetrais. Em caso de alarme de intrusão, deve ser indicado em qual área ocorreu a intrusão e qual porta ou perímetro foi violado, direcionando o trabalho do operador e da equipe de segurança patrimonial, de acordo com os procedimentos de segurança desenvolvidos. Assim, se faz recomendável que o sistema de Monitoração e Inteligência Predial tenha a repetição de, no mínimo, os seguintes eventos: *status* de porta aberta; alarme de violação da porta; alarme de sensor “anticarona”; alarme de violação da área perimetral; alarme acionamento de botão de saída de emergência; integração entre o sistema de controle de acesso e o de monitoração e tratamento de imagens, permitindo que qualquer ocorrência anormal ative uma câmera de TV e mostre na tela do sistema a imagem do local do evento, facilitando o trabalho do pessoal de segurança.

No sistema para Detecção e Combate a incêndio devem ser monitorados os parâmetros integrados ao sistema de Monitoração e Inteligência Predial da mesma forma que o sistema de Acesso e Intrusão, deste modo, todo e qualquer alarme de incêndio, seja ele a partir dos detectores convencionais de fumaça e temperatura ou pelo sistema de detecção precoce à incêndio, devem ser imediatamente transferidos para que o operador tome medidas preventivas ou corretivas de combate à incêndio. O sistema deve possuir interface de comunicação, de tal modo que todas as áreas abrangidas pelo sistema de detecção e combate sejam representadas em telas gráficas, indicando o posicionamento dos detectores convencionais de fumaça e temperatura e os detectores a laser (detecção precoce). Em caso de detecção de

incêndio, o sistema de Monitoração e Inteligência Predial deve indicar em qual área ocorreu a detecção de incêndio e qual o detector (convencional ou laser) foi acionado, direcionando o trabalho do operador e da Brigada de Incêndio e supervisionando o *status* dos sistemas de combate a incêndio e monitorando o acionamento de cabeças de disparo de gás, de *dumpers* corta-fogo e ou anomalias na rede elétrica de distribuição, além de sinais de defeito do sistema, funcionando como um painel repetidor da central de detecção e combate a incêndio.

Na Detecção de Vazamento de Líquidos devem ser monitorados os parâmetros, de modo que, todo e qualquer alarme deve ser imediatamente transferido ao sistema de Monitoração e Inteligência Predial para que o operador tome medidas preventivas ou corretivas para conter o vazamento de água. O sistema deve possuir *interface* de comunicação, de tal modo que todas áreas abrangidas pelo sistema de detecção de líquidos sejam representadas em telas gráficas, indicando o posicionamento do cabo detector de líquido. Em caso de detecção de vazamento, deve indicar em qual localização da área ocorreu o vazamento, direcionando o trabalho do operador e da equipe de manutenção. O sistema também deve supervisionar o *status* do sistema de detecção de vazamento, monitorando anomalias na rede elétrica de distribuição e sinais de defeito do sistema, funcionando como um painel repetidor da central de detecção de vazamento de líquidos.

No Ar-condicionado devem ser monitorados todos os equipamentos que compõem o sistema, monitorando o funcionamento, condições de temperatura e umidade dos ambientes e alteração de parâmetros de funcionamento (*set points* de temperatura e umidade e alteração no escalonamento do rodízio entre equipamentos). O sistema que faz o controle dos equipamentos de ar-condicionado deve possuir *interface* de comunicação, de tal modo que toda a área abrangida seja representada em telas gráficas, indicando o posicionamento dos equipamentos e o *status* de funcionamento deverá ser representado através de telas gráficas, de fácil visualização para o operador. Em caso de qualquer alarme, o sistema deve indicar em qual área ocorreu a alteração de *status* ou alarme, direcionando a atuação do operador e da equipe de manutenção. Assim, torna-se desejável que o sistema tenha o gerenciamento e monitoramento de, no mínimo, os seguintes eventos e/ou funções: alteração de *set*

points de temperatura e umidade; alteração da programação horária do rodízio entre equipamentos; visualização dos valores ambientes de temperatura e umidade, em tempo real; *status* de funcionamento de ventiladores, compressores, sistemas de aquecimento e umidificação; alarme de defeito de equipamento; alarme de filtro sujo; alarme de alta ou baixa temperatura; alarme de alta ou baixa umidade; alarme de falha de umidificador.

Nos sistemas auxiliares de iluminação, água potável, ventilação/exaustão, motores e bombas, a Monitoração e Inteligência Predial deve efetuar os controles de modo a comandar : o ligamento e desligamento das luzes em função de horário, do nível de iluminação externa, da presença de pessoas nos ambientes e controle de demanda, sendo que, os painéis elétricos de iluminação devem ser providos de contadoras telemonitoradas e comandadas, contando também com sensores de presença instalados no ambiente e sensores fotoelétricos instalados nas áreas externas; o monitoramento dos volumes dos reservatórios, alarmando quando estes níveis estiverem críticos, sendo que este deve ser efetuado através de medidores analógicos que deverão possuir interface com o sistema; o adequado funcionamento dos diversos sistemas de ventilação/ exaustão, alarmando os seguintes eventos - falha no funcionamento do ventilador/ exaustor, alarme de problema nas condições ambientes requeridas (sobre temperatura, alta concentração de fumaça ou partículas, etc); o funcionamento de motores e bombas instalados para funcionamento das utilidades do prédio do CPD, para tanto, devem ser instalados sensores e controles enviando sinais analógicos e digitais para o sistema, tendo as seguintes funções - ligamento e desligamento de motores/ bombas, conforme necessidade ou programação horária, status de funcionamento dos motores/ bombas, supervisão de alarmes de defeito, supervisão de chaves manuais/ automáticas e escalonamento automático de funcionamento para homogeneizar o desgaste dos equipamentos.

Ao final deste capítulo, podemos verificar que as especificações de padrões prediais confiáveis são muito complexas e detalhadas, as quais devem ser desenhadas com a maior atenção pelos gestores de *Facilities* em CPD's, portanto, precisam ser alvo de um modelo de governança específica.

Capítulo 5 – REQUISITOS CONTRATUAIS AOS FORNECEDORES

Neste capítulo, há um enfoque das análises em considerações quanto aos Contratos e o Gerenciamento de Facilidades, evidenciando que, historicamente houve uma flexibilização da auto-suficiência predominante nas empresas até a década de 80. Assim, a partir da década de 90 as necessidades de rapidez na adaptação às transformações e de agilidade para reação às crises, os surtos de crescimento e as situações de riscos, fizeram emergir processos de *joint-ventures*, consórcios e a terceirização de serviços, presentes até os dias atuais e que são fonte de muitos problemas quando não tratados de forma adequada.

Por definição, contrato é o acordo de vontades onde as partes livremente estabelecem direitos e deveres recíprocos, o qual possui algumas fases distintas que podemos identificar, conforme segue : constatação das necessidades; diagnóstico (estabelecimento e identificação de padrões, especificações e outros); negociação; pré-contratação; acompanhamento da execução; satisfação das necessidades; vencimento/distrato.⁴⁴

O enfoque principal do presente capítulo recai sobre a fase de constatação das necessidades do contrato, na qual incluem-se questões quanto ao objeto (o quê?), destino (para quem? – os clientes do contrato), foco econômico-financeiro (quanto? quando?), foco técnico (como? quando? – a modalidade de satisfação das necessidades e o prazo de cumprimento), as garantias e as condicionantes, sendo que, nestas três últimas questões temos a essência das considerações desta abordagem sobre os requisitos contratuais aos fornecedores.

Dentre as mais variadas espécies (tipos), estruturas, cláusulas e classificações de contratos, a formalização de um texto contratual permite a reconstituição do mapa de intenções, relembra a outra parte do que foi estabelecido, afasta a possibilidade da diversidade de impressões/interpretações/subjetividades e previne a existência de

distorções. Os dois pontos principais do contrato neste capítulo são essencialmente técnicos – a qualificação dos fornecedores e os aspectos técnicos dos serviços. As características referentes às obrigações das partes são estabelecidas basicamente por meio de dois tipos de documentos nos quais constam as diretrizes básicas para as solicitações de propostas e coletas de informações dos proponentes – a *RFP-Request for Proposal* e a *RFI-Request for Information*.

Portanto, todos os materiais, equipamentos, sistemas e serviços fornecidos pelos fabricantes, contratados e/ou sub-contratados, devem estar em conformidade com as especificações dos cadernos de recomendações e diretrizes para o fornecimento, em cumprimento aos itens constantes das respectivas *RFP-Request for Proposal* e *RFI-Request for Information* (memoriais descritivos para coleta de informações dos concorrentes e diretrizes básicas para as solicitações de orçamentos), as quais devem ser elaboradas visando estabelecer os requisitos básicos de fornecimento que podem abranger os seguintes pontos: fornecimento de desenhos de fabricação para aprovação prévia; compromisso de qualidade; garantias; desenhos finais e diagramas; testes e ensaios de fábrica; entrega de armazenagem e manuseio; manutenção; peças de reposição; treinamento; supervisão de montagem; controle de qualidade de campo; testes de aceitação em campo; assistência ao comissionamento.

Os desenhos de fabricação devem ser elaborados por todos os fornecedores de equipamentos, com base no escopo efetivamente contratado, e devem indicar, com medidas em vistas e plantas, no mínimo o seguinte: dimensões do equipamento; peso do equipamento e distribuição do peso nos apoios; centro de gravidade (eixos X e Y); planta inferior, com apoios e indicação das janelas para entrada/ saída de utilidades; planta superior, com indicação de janelas para entrada/ saída de utilidades; planta baixa com espaços mínimos necessários para manutenção e serviços; bitolas máximas e mínimas de bornes para conexões elétricas; indicação de diâmetros e tipos de roscas para conexões hidráulicas; recomendações para transporte. Além disso, devem ser fornecidas informações técnicas sobre o equipamento, tais como: tensão e frequência de trabalho; consumo elétrico e fator de potência; nível de ruído gerado a plena carga; distorção harmônica, se equipamento

eletrônico; dissipação térmica e temperatura de operação; outras que o fabricante julgue necessárias à elaboração do projeto de instalação.

O fornecedor deve assumir um compromisso de qualidade que inclua manter um centro de serviços que permita executar uma manutenção de emergência ou reparo em no máximo 8 horas, utilizar componentes certificados por laboratórios ou entidades de renome internacional, estar em conformidade com as normas locais se internacionais aplicáveis ao tipo do produto, garantia de cumprimento às normas de emissão de gases/ poluentes, bem como o atendimento aos níveis máximos de ruído aceitáveis para legislação local, na contratação de execução de serviços, o nível de SLA-*Service Level Agreement* (Acordo do Nível de Serviços) determinado por ocasião do pedido deve ter o programa SLM-*Service Level Management* (Gerenciamento do Nível de Serviço) detalhado e seus controles e indicadores colocados à disposição do cliente. O compromisso de qualidade de serviço dos fornecedores deve ser completado com o Aceite Preliminar executado pelo Gerenciador e da empresa Comissionadora.⁴⁵

O fornecedor deve ofertar, no mínimo, a garantia exigida no pedido podendo, contudo, apresentar uma garantia maior ou opção de garantia estendida. A garantia deve indicar, ainda, o compromisso de manutenção de peças de reposição em estoque por um período mínimo de 5 anos e o tempo de atendimento e de reparo em caso de emergência. Na execução de serviços, a garantia deve abranger o seguinte: o disposto no Código Civil Brasileiro onde aplicável; o disposto no CDC-Código de Defesa do Consumidor; garantia mínima de 1 ano contra vícios ocultos, isto é, aqueles cujo diagnóstico somente pode ser percebido após o uso continuado das instalações, com esta finalidade, deve ser executado o Aceite Final após 1 ano da instalação; independente das garantias apresentadas o fornecedor deve apresentar seguro de risco de engenharia com cobertura que abranja inclusive erros de projeto.

Após o fornecimento, a empresa deve apresentar os desenhos finais e diagramas elétricos e de comando para o objeto do fornecimento, incorporando eventuais alterações ocorridas no processo de produção. Quando aplicável, os fornecedores de

serviços devem apresentar na fase de entrega, os manuais de utilização e conservação e instruções de uso nas situações normais e emergenciais. Os equipamentos que, por exigência do pedido, sejam testados em fábrica devem ter o roteiro de testes submetido à aprovação do gerenciador e do cliente previamente aos testes. Pode ser designada a equipe de acompanhamento aos testes em fábrica, a critério da contratante. Recomenda-se o teste de fábrica para no mínimo os equipamentos abaixo relacionados: grupos moto-geradores; UPS e respectivos bancos de baterias; chaves estáticas (STS); chaves de transferência (ATS); transformadores; cubículos de média tensão; painéis elétricos de baixa tensão. Independente dos testes serem ou não testemunhados pelo cliente ou seus prepostos, o fornecedor deve entregar as folhas de testes com os respectivos resultados, conformidades e desvios ao gerenciador e ao cliente, junto com a entrega dos equipamentos.

O fornecedor deve ser responsável pela entrega, armazenagem e manuseio do equipamento no local da instalação, até sua efetiva conclusão. Danos ao equipamento devem ser reportados ao cliente e ao fornecedor, a quem cabe a definição sobre sua substituição ou não. Os equipamentos devem ser embalados adequadamente, para evitar danos no transporte, e mantidos assim até sua colocação no local definitivo da instalação. As embalagens devem possuir “fusíveis de choque” que indicam a ocorrência de choques no transporte. A embalagem somente deve ser removida após o ambiente da instalação estar limpo, livre de pó, umidade ou outros fatores agressivos ao conteúdo.⁴⁶

O fornecimento dos equipamentos deve prever um contrato de manutenção pelo período de 1 (um) ano, a partir do *start-up* (ativação) e aceitação dos mesmos, com peças de reposição incluídas. Como já citado, a manutenção deve incluir tempos máximos para atendimento e reparo. O Fornecedor deve indicar, relacionar e apresentar custos para um estoque mínimo de peças de reposição a serem adquiridas pelo cliente, com o objetivo de reduzir os tempos de paralisações do funcionamento dos equipamentos. Após os testes de aceitação, o fornecedor deve efetuar um treinamento teórico e prático para os operadores da infra-estrutura do CPD. Este treinamento, deve ser realizado nas instalações do cliente, utilizando-se de apostilas e

manuals de manutenção e operação em português. No treinamento, o fornecedor deve entregar os seguintes documentos: lista de ferramentas recomendadas para serem mantidas no site visando os procedimentos de manutenção; instruções detalhadas de operação em condições normais ou anormais, em língua portuguesa.

Caso se julgue necessário, pode ser solicitado ao fornecedor a presença de equipe de técnicos de montagem para supervisionar, orientar e esclarecer eventuais dúvidas que podem surgir durante a montagem ou instalação dos equipamentos. Após a conclusão da montagem, o fornecedor deve enviar ao campo um supervisor técnico responsável pela verificação e aceitação da instalação, sua conformidade com os manuais e desenhos fornecidos, liberando o equipamento para testes. Deve ser elaborado um relatório indicando as condições aceitáveis de instalação ou notificando eventuais itens a serem cumpridos para permitir o início dos testes. Os testes somente podem ser iniciados após a formalização da liberação pelo preposto do fabricante. A aceitação final dos equipamentos ou sistemas fornecidos deve ocorrer após os testes em campo, sendo que, o fornecedor deve providenciar os equipamentos necessários aos testes e submeter o roteiro dos mesmos à aprovação da contratante para análise prévia. Após a conclusão da instalação, o fornecedor deve disponibilizar equipe técnica qualificada, de seu quadro de funcionários, para supervisionar e prestar assistência à equipe de comissionamento. O gerenciador deve comunicar a data ao fornecedor com no mínimo 5 dias de antecedência, sendo que, o cliente, o gerenciador, o fornecedor e a comissionadora devem reunir-se previamente para estabelecer um roteiro aceitável para os testes. Todos devem ser responsáveis pelo acompanhamento dos testes até a aceitação.⁴⁷

5.1 Projetos Conceituais e Executivos

A equipe de coordenação técnica do cliente ou seus prepostos devem estabelecer em um documento formal, todas as necessidades volumétricas/espaciais, de infraestrutura, as redundâncias e a segurança desejadas para o projeto do CPD, sem,

contudo haver uma maior preocupação naquele momento com o desenho destas soluções. Neste momento, deve ser contratado um trabalho chamado *Projeto Conceitual*, onde a empresa escolhida deve desenvolver a aplicação das soluções definidas no documento anterior à realidade das necessidades e disponibilidades do cliente, por meio de Dimensionamentos, Memoriais, Plantas, Esquemas e Desenhos Técnicos que tenham como resultado uma Definição Perfeita das Soluções, um Cronograma Preliminar e uma Estimativa dos Custos Envolvidos, por Sistemas, Sub-sistemas e Global, para execução do CPD. Com base na solução aprovada no *Projeto Conceitual* deve ser contratado pelo cliente um *Projeto Executivo*, no qual devem ser detalhadas todas as soluções adotadas no Projeto Conceitual para se obter um resultado absolutamente exequível em todos os seus aspectos técnicos, onde devem constar (nos mínimos detalhes) especificações, plantas, memoriais aprovações legais e demais produtos, oferecendo o material adequado e suficiente para uma pronta contratação para execução de Obras, conforme Tabela 5 a seguir.

Tabela 5 – Descritivo Básico das Principais Atividades dos Projetos

Fonte : AUTOR

Projeto Conceitual	Projeto Executivo
Estudo Preliminar / Anteprojeto de Arquitetura	Projetos Técnicos (Civil, Hidráulica, Elétrica, Climatização, etc.)
Projeto Conceitual de Civil	Projeto Legal / Projetos de Execução
Projeto Conceitual de Elétrica	Compatibilizações / Detalhamentos
Projeto Conceitual de Hidráulica	Caderno de especificações
Projeto Conceitual de Climatização	Caderno de Imagem / maquetes
Projeto Conceitual de Segurança, Detecção e Combate a Incêndio	Acompanhamento / apoio à equipe de Comissionamento
Projeto Conceitual de Automação	Planilhas de quantitativos preliminares

	Escopo da Empresa de Arquitetura
	Escopo da Empresa de Engenharia

O Projeto Conceitual deve constituir-se de um refinamento e aprovação aos conceitos e diretrizes preliminares do Projeto Básico do cliente, transformando-o em solução para a posterior contratação e execução de um Projeto Executivo que deve produzir a integração dos projetos de infra-estrutura específicos (Civil, Elétrica, Mecânica, Climatização, Segurança, dentre outros) com os Projetos de Arquitetura e Civil incluindo todos os detalhes suficientes e necessários para a execução do espaço construído, a operação e manutenção do CPD, conforme detalhamentos que constam dos itens a seguir :

- GERAL / CIVIL : Definição das áreas para todas Utilidades e Infra-estruturas; Estudo de Solos / Fundações; Pré-dimensionamento de Lajes e Vigas; Pré-dimensionamento de Estruturas e Fundações;
- ELÉTRICA / HIDRÁULICA / CLIMATIZAÇÃO : Cálculos das Cargas Elétricas, Térmicas, Dissipação, Ventilação, Exaustão, Vazão e Iluminação, entre outros; Dimensionar Componentes, Equipamentos e Sistemas; Definição final das Tecnologias e Sistemas;
- SEGURANÇA , DETECÇÃO E COMBATE A INCÊNDIO E AUTOMAÇÃO PREDIAL : Definir Locais e Tipos de Sistemas; Perimetral; Controle de Acesso e Intrusão; CFTV; Detecção e Combate à Incêndio; Detecção de Vazamentos; Alarmes e Monitoramento; Controle de Temperatura e Umidade; Controle de Energia e Consumo.

Como instruções gerais aos concorrentes à execução dos projetos podem ser considerados os seguintes pontos : A Empresa vencedora da Proposta para execução do Projeto Conceitual não pode participar da licitação para Gestor da Execução ou Execução da futura da obra; As empresas que possuem Certificação ISO-9000 ou estiverem em processo de obtenção da certificação podem obter um diferencial na avaliação geral do processo licitatório; A proponente deve apresentar as suas qualificações profissionais incluindo a de seus parceiros mediante Atestados de Referência atendendo aos seguintes pré-requisitos : listar experiência em projetos e consultoria na área de *Datacenter* para Missão Crítica; comprovar elaboração de Projetos Conceituais na área de Missão Crítica, de preferência em organizações financeiras, no Brasil e exterior; experiência em Projetos de instalações de sistemas

elétricos de alta potência e alta disponibilidade em sites de missão crítica; experiência em projetos de Sistemas Redundantes do tipo “*Dual Bus*” e “*Three Bus*” para distribuição elétrica em *Data Centers*; experiência em projeto de sistemas de combate à incêndio via gases inertes, “*dry-sprinkler*” e sistemas de Detecção Precoce com laços cruzados e integrados à detecção convencional com Inteligência Artificial; experiência comprovada em projetos de Climatização de Precisão para *Data Center* com alto teor de carga térmica de calor sensível; experiência comprovada em projetos de sistemas de suporte para *Data Center* com utilização de UPS, PDU, STS/ATS, TVSS e sincronismo de UPS mediante apresentação de diagramas unifilares executados; experiência comprovada em projetos de Sistemas de Geração de Energia em grupos moto-geradores em um mesmo Site, incluindo-se neste item também os projetos dos sistemas de armazenamento, conservação, distribuição e controle automático de óleo diesel; experiência comprovada em projetos de Sistemas de Automação e Controle (BAS/BMS) para instalações desse porte; os concorrentes devem possuir representante ou parceiro local, no Brasil, atuante na área de projetos, apresentando atestados que comprovem a elaboração de Projetos de Missão Crítica, de preferência em organizações financeiras, no Brasil e no exterior; as atividades e projetos citados pela proponente devem obrigatoriamente estar acompanhados de Atestados de Referência; no caso de não participação ou abandono da concorrência, todos os documentos enviados devem ser imediatamente devolvidos, acompanhados de uma notificação com o motivo do declínio; a apresentação de proposta deve implicar na aceitação de todos os termos da concorrência, salvo eventuais ressalvas claramente definidas na mesma; todas as despesas ou ônus de qualquer natureza incorridos na elaboração das propostas, como por exemplo, custos decorrentes de levantamentos, reuniões, horas técnicas de profissionais, viagens ou locomoção, são de responsabilidade exclusiva do proponente; o proponente deve se comprometer a manter a devida confidencialidade do conteúdo e das informações contidas na concorrência, mediante assinatura do termo de confidencialidade; qualquer sugestão de alteração/modificação nos conceitos apresentados em diretrizes ou em Projeto Básico do cliente, visando embasar a elaboração do Projeto Conceitual, devem ser submetidos à avaliação e aprovação prévia da equipe técnica de avaliação dos projetos, designada pelo cliente; documentações comprobatórias de situação regular

nos aspectos comerciais (CND-Certidão Negativa de Débitos, ART-Anotação de Responsabilidade Técnica, Aderências às Legislações Pertinentes, Habilitações de Profissionais Especializados, dentre outras).⁴⁸

5.2 Gerenciamento da Construção e Montagens

O Gestor da Construção constitui-se da empresa responsável pelo gerenciamento, dos recursos, dos fornecedores e sub-contratados que são parte da construção do CPD, a qual deve realizar os melhores esforços para garantir o cronograma da obra, os níveis de qualidade definidos em projeto, o cumprimento do orçamento definido pela equipe de coordenação técnica do cliente ou seus prepostos, além de acompanhar e aceitar a obra. A atuação do Gestor da Construção deve se dar em três grandes áreas de atividade do Projeto - Pré Construção, Construção, Entrega e Aceite da Obra.

As atribuições do Gestor da Construção devem ser estabelecidas conforme descrição contida nos itens a seguir :

- ◆ **Fase de Pré Construção :** apoio técnico na execução dos Orçamentos de Obra; identificação de potenciais fornecedores; elaboração de RFP's; programação de atividades e recursos; análise e depuração de Sistemas Críticos relativos ao projeto; equalização e análise de propostas;
- ◆ **Fase de Construção :** controle financeiro; fiscalização técnica de Obras, Instalações e Sistemas; inspeção e controle de Qualidade; cronogramas gerais para Elaboração, Implementação e Controle; reuniões técnicas em geral, Gerenciais e de Progresso; controle de documentação técnica em geral; recebimento de equipamentos em fábrica; medições de serviços executados, liberação e controle de pagamentos

- ♦ **Fase de Entrega e Aceite de Obra :** acompanhamento de Testes Integrados; acompanhamento do Comissionamento de Equipamentos e Instalações; Pré-requisitos para a prestação dos serviços.

A empresa candidata a Gestor de Construção do CPD deve atender, no mínimo, aos seguintes pré-requisitos : corpo técnico de Engenharia e Arquitetura com experiência comprovada no segmento de projetos de Sistemas e Ambientes de Missão Crítica; experiência comprovada de participação em obras de CPD de Missão Crítica, com características similares ao CPD sob enfoque das cotações para a prestação de serviços especializados, com trabalhos efetuados que evidenciem a aplicação de várias soluções de mercado para as instalações prediais; registro no CREA; dispor de responsáveis técnicos em seu quadro de funcionários com experiência comprovada nas áreas de construção civil, instalações elétricas, de ar condicionado de precisão / ventilação, de segurança patrimonial, de CFTV , de controle de acesso, de combate a incêndio, *dry sprinklers*, detecção de fumaça convencional / precoce e de supervisão predial; atestados, com registro no CREA e seus respectivos Acervos Técnicos para obras com as seguintes características e equivalente ao cotado - Instalações de Grupos Geradores compatíveis em potência em um mesmo site; Instalações Elétricas para CPD de potência instalada compatível em um mesmo site; Instalações de Ar-condicionado de expansão direta com unidades microprocessadas para CPD, compatível em um mesmo site; Sistemas de armazenamento e distribuição de Óleo Combustível compatível em um mesmo site; Instalações de Combate a Incêndio com Gases Especiais, Sistemas de Detecção Normal e Precoce de Incêndio; Sistemas de Supervisão Predial integrados; experiência internacional na elaboração de trabalhos similares, quer por sua equipe própria, quer através de acordos formais de parcerias e transferência de tecnologia em CPD's e projetos desta natureza; Conhecer as exigências de certificação internacional de edificações dessa natureza; Demonstrar capacidade atualizada de tecnologia de coordenação para projetos multidisciplinares; Apresentar Curriculum Vitae dos profissionais a serem envolvidos no Projeto, bem como diagrama da estrutura de pessoal a ser utilizada, indicando cargo, local de trabalho e carga de trabalho; Fornecer atestados que comprovem a experiência e

idoneidade da empresa, tempo de existência no mercado e situação financeira corrente.

A empresa responsável pelo gerenciamento da obra, incluindo seus recursos, fornecedores e sub-contratados, deve realizar os melhores esforços para garantir o cronograma da obra, os níveis de qualidade definidos em projeto, o cumprimento do orçamento definido pelo cliente e seus prepostos, além de acompanhar e aceitar a obra. A atuação do Gerenciamento da Construção deve se dar nas fases do projeto descritas a seguir : Pré-Construção; Construção; Entrega e aceite da obra; Plano de Migração e Início de Operação (pode ser tratado em um contrato específico para este fim).

As atribuições do Gerenciamento da Obra em cada fase pode ser dividido da seguinte forma : **Fase de Pré-Construção** (acompanhamento, análise e parecer dos projetos de arquitetura e engenharia; elaboração da previsão orçamentária da Obra; identificação de potenciais fornecedores de equipamentos e serviços; elaboração de cartas dirigidas às empresas contendo as observações para ratificação do escopo técnico não identificado na planilha; elaboração da Documentação Técnica necessária para tomada de preços, com base nas especificações e memoriais dos projetistas: Memoriais Descritivos; Levantamento Quantitativo dos Serviços; Detalhes Técnicos; Minuta de Contrato; Caderno de Encargos; Cronograma Físico Financeiro e outros; atendimento aos participantes das concorrências, em conjunto com o cliente, visando dirimir dúvidas; elaboração da programação de atividades e recursos; análise e equalização orçamentária de todas as propostas técnicas e comerciais; elaboração de relatórios contendo a planilha orçamentária de custo da gerenciadora e todas demais informações técnicas necessárias observadas na análise da (s) proposta (s), para subsidiar a negociação da obra pelo Contratante; participação da negociação, elaboração de ata conforme condições técnicas e financeiras pactuadas; elaboração de “Caderno Resumo” do processo de concorrência, contendo toda documentação técnica e análise orçamentária); **Fase de Construção** (programação detalhada de Atividades e Recursos; estudo de compatibilização dos Projetos Executivos, verificando possíveis interferências e

analisando alternativas não previstas no Projeto, com justificativas em forma de relatórios técnico e fotográfico; elaboração de Memorial Descritivo de serviços necessários, conforme levantamento e Projetos Executivos já adequados às necessidades locais e previamente aprovados pelo Contratante; elaboração de Cartas Convite com sugestões de empresas ao Contratante para os processos de concorrência; elaboração da Documentação Técnica necessária para tomada de preços com base nas especificações e memoriais dos projetistas; Memoriais Descritivos; Levantamento Quantitativo dos Serviços; Detalhes Técnicos; Minuta de Contrato; Caderno de Encargos; Cronograma Físico Financeiro e outros; atendimento aos participantes das concorrências, em conjunto com o cliente, visando dirimir dúvidas; participar da análise e equalização orçamentária de todas as propostas técnicas e comerciais com a elaboração dos relatórios contendo as planilhas orçamentárias de custo meta da gerenciadora e todas as demais informações técnicas necessárias; cartas dirigidas às empresas contendo as observações para ratificação do escopo técnico não identificado na planilha; participação da negociação, elaboração de ata conforme condições técnicas /financeiras pactuadas; elaboração de “Caderno Resumo” do processo de concorrência, contendo toda documentação técnica e análise orçamentária; análise e aprovação de cronograma físico financeiro; elaboração de todo o planejamento da obra, bem como rede de procedência em conjunto com as Empresas Contratadas, Subcontratadas, Fornecedores e Órgãos Públicos / Concessionárias; negociar com empresas construtoras, instaladoras e fornecedores os melhores prazos e custos para a Contratante sempre que for necessário e cabível; planejamento e programação com todos os Setores, Departamentos do Contratante e Fornecedores envolvidos direta ou indiretamente na obra; coordenar junto aos Setores, Departamentos e Fornecedores envolvidos, responsabilidades e programações, visando atingir as metas de atendimento de prazos e metas estabelecidas pelo Contratante; gestão da documentação técnica, relacionando, mantendo em arquivo físico e eletrônico, disponibilizando e garantindo que todos os envolvidos estejam trabalhando com as ultimas versões homologadas de projetos, memoriais e especificações técnicas, via Web e com disponibilização/gerenciamento de normas nacionais e internacionais aplicáveis ao CPD; controle da elaboração e emissão de “As Built”; fiscalização dos serviços

contratados e subcontratados, bem como assegurar a qualidade e o fiel cumprimento dos projetos aprovados, especificações, normas técnicas e metas estabelecidas; fiscalizar o cumprimento de normas estabelecidas pelo Ministério de Trabalho, com especial atenção de Norma Regulamentadora (NR), relativas à Higiene, Medicina e Segurança do trabalho; análise técnica especializada para serviços e equipamento específicos, tais como, Sistemas Elétricos, Ar Condicionado, Lógica, Aterramento, Transformadores, Elevadores, Supervisão e Automação Predial, Controle de Acesso e CFTV, dentre outros; contratação de ensaios de controles tecnológicos especializados e pareceres técnicos, quando necessários, com ênfase nos ensaios das instalações elétricas de baixa tensão via instrumentação específica para a emissão de avaliação de conformidade com a norma NBR5410:2004; promover reuniões de esclarecimento de dúvidas e alternativas técnicas, junto às empresas de projetistas, construtora, instaladoras e demais contratadas; acompanhamento da realização de testes em fábrica de equipamentos tais como UPS, transformadores, ar condicionado, dentre outros, sempre que solicitado pelo cliente; promover reuniões para tomada de decisões com o Contratante; participação em reuniões periódicas, no mínimo semanal, nas dependências do cliente, com Setores e Departamentos envolvidos nos eventos, visando o monitoramento; coordenação de cronogramas de entrega de materiais e equipamentos utilizados na obra, visando o atendimento e realização dos serviços dentro dos prazos previstos no Cronograma Físico Financeiro e Rede de Precedência; definição de metas de controle e acompanhamento para recuperação de eventuais atrasos ocorridos, ou que venham a ocorrer; emissão de relatórios técnico/financeiro para prévia aprovação do Contratante, de serviços extracontratuais; análise e acompanhamento de serviços extracontratuais, aprovados pelo Contratante e seus prepostos; controle sobre os processos de aprovações legais junto aos Órgãos Públicos e Concessionárias, bem como as vistorias relativas a estes; relatórios técnicos, financeiros, fotográficos, cronograma e medição da evolução da obra semanalmente, bem como demais documentos de gerenciamento com disponibilidade de consulta via internet, mediante os cuidados de segurança para acesso a dados em sistema de proteção com senha e *log* de acesso em site seguro; medições dos serviços executados conforme “modelo padrão” a ser definido para efeito de liberação de parcelas, conforme Cronograma Físico Financeiro aprovado;

elaboração de relatórios de gerenciamento, contemplando histórico do período, fotos, gráficos, relatórios de fiscalização, medições, correspondências, *as-built*, protocolos de documentação de concessionárias e órgãos públicos, cópia do diário de obra, dentre outros; acompanhamento do Comissionamento de Equipamentos e Instalações; elaboração do *check-list* final da obra enfocando todas as etapas e serviços concluídos conforme projetos, especificações, normas técnicas e memoriais descritivos e aceite provisório da obra); **Fase de Entrega e Aceite de Obra** (acompanhamento de Testes Integrados; acompanhamento e Finalização do Comissionamento de Equipamentos e Instalações; aceite final da obra, mediante análise da documentação exigida em contrato e memorial descritivo, manuais e certificados de garantia, certidões, ART's, documentos circunstanciais e aprovações em concessionárias e órgãos públicos; encerramento do *check-list* final da obra; coordenação, elaboração e entrega do Plano de Operação e Manutenção do site, bem como a coordenação de treinamento das equipes responsáveis; Plano de Migração e Início de Operação).

As empresas com Certificação ISO-9000 ou que estiverem em processo de obtenção da certificação, devem receber diferencial na avaliação da proposta. Quando empresas estrangeiras forem proponentes devem possuir representante ou parceiro local, no Brasil, e apresentarem atestados que comprovem o gerenciamento de Construções de Missão Crítica, de preferência em organizações financeiras, no Brasil e no exterior. No caso de não participação ou abandono de concorrência, todos os documentos enviados devem ser imediatamente devolvidos, acompanhados de uma notificação com o motivo do declínio pelo concorrente. O proponente deve se comprometer a manter a devida confidencialidade do conteúdo e das informações contidas na concorrência, mediante assinatura de termo de confidencialidade. Qualquer sugestão de alteração/modificação nos Conceitos apresentados no “Projeto Executivo do CPD”, devem ser submetidos à avaliação e aprovação de um Conselho formado pelos prepostos indicados pelo cliente. A qualquer tempo devem prevalecer as normas técnicas vigentes (ABNT, dentre outras) e os requisitos básicos do memorial descritivo para base de cotações, sendo que nos casos onde as normas forem omissas, conflitantes e/ou divergentes deste, devem ser adotadas as soluções

tecnicamente mais perfeitas, cabendo a aprovação e decisão final à fiscalização designada pelo cliente e seus prepostos.

5.3 Cronograma, Qualidade e Garantias

O alto nível de competitividade em que as organizações se encontram exige que as melhores técnicas de gerenciamento sejam aplicadas e que estas sejam amparadas por ferramentas adequadas. Através de uma orientação única e respaldada pelas práticas do *PMI-Project Management Institute*, este tópico envolve os recursos e as três áreas básicas do conhecimento para controle de um projeto – escopo, tempo e custo. A visão PMBOK 2004 – *A Guide to the Project Management Body of Knowledge* – NBR ISO 10006, envolve a apresentação das melhores técnicas de gerenciamento de projetos, fazendo entender a maior abrangência da palavra “Projeto” ao definir um “serviço único e individual que produz um resultado único, utilizando-se de recursos materiais, humanos e financeiros limitados, a ser entregue aos clientes dentro de especificações claras, na qualidade adequada”. Assim entendido, o projeto abrange três conjuntos básicos de atividades : ³⁰

- ♦ **Controle físico do projeto** : elaboração do Termo de Abertura do projeto; elaboração dos documentos iniciais do projeto; elaboração, criação e inclusão de arquivos; elaboração do dicionário, criação de modos e tabela; elaboração de organograma; criação de visões – grupos; elaboração da lista de atividades dos pacotes de trabalho; sequenciamento de atividades; inclusão da lista de atividades dos pacotes de trabalho; definição das restrições e premissas das atividades; apresentação do diagrama de rede do projeto; definição da duração das atividades – marcos do projeto; definição dos calendários; elaboração do cronograma do projeto – base de referência de tempo;
- ♦ **Controle dos recursos do projeto** : criação e administração do grupo de recursos – *pool* de recursos; análise da alocação dos recursos; análise do uso dos

recursos nos produtos principais; análise da superlocação dos recursos e seus custos;

- ♦ **Controle financeiro do projeto** : análise dos custos fixos e do orçamento do projeto; elaboração de uma proposta de redução de prazo e custo no projeto; trabalho consolidado – integração e desempenho de projeto; trabalho final de planejamento integrado – projetos e subprojetos; análise do valor do trabalho realizado.

O cronograma deve abranger todos os ambientes de Missão Crítica para TI, visando atender as necessidades do CPD no Site Principal, Cabine de Comando e as melhorias do Site Back-up (obs: ambiente de contingência). O trabalho de planejamento da migração física e de sistemas também deve ser iniciado antecipadamente, considerando todos os fatores envolvidos como equipes, equipamentos, necessidade financeira, disponibilidade, distâncias, riscos, qualidade e responsabilidade. A estratégia para a migração deve ser elaborada e validada com todas as partes envolvidas para obtenção e clareza dos objetivos propostos, sendo que, devem ser considerados os seguintes aspectos:

- **Planejamento** : Criação do plano de trabalho; Levantamento da situação atual; Definição de estratégia geral de migração (físico e lógico); Definição do cronograma geral; Definição do cronograma financeiro; Definição das equipes envolvidas; Definição da matriz de responsabilidades; Definição do plano de comunicação; Definição de matriz de riscos e mitigação; Definição de métricas e indicadores de qualidade;
- **Migração** : Detalhamento do plano de migração; Validação dos ambientes futuros (capacidade de processamento e armazenamento);
- **Projeto Físico** : Elaboração do plano de conexão física; Validação do layout físico para os equipamentos; Verificação da adequação da infra-estrutura física; Roteiro para implementação física;
- **Projeto Lógico** : Elaboração do plano de conexão lógica; Roteiro para implementação lógica;

- **Definição da estratégia de *roll-back* (*back-up*)** : Elaboração do plano de *roll-back*; Roteiro para implementação do plano de *roll-back*;
- **Testes e validação** : Elaboração do plano de testes; Elaboração do roteiro de testes; Definição de métricas para validação.

O sucesso da implementação de projetos desta natureza pode ser diretamente ligado à capacidade que as pessoas têm em aceitar e praticar os novos modelos. Para garantir a consecução de seus objetivos, deve ser promovido um programa de Gerenciamento da Mudança (*Change Management*), englobando não somente aspectos técnico-organizacionais mas também, comportamentais. Neste programa devem ser considerados os seguintes aspectos: Gerenciamento da Mudança; Estratégia de Alinhamento; Estratégia de Comunicação e Envolvimento (Plano de Comunicação e Plano de Envolvimento); Estratégia de Treinamento.

5.4 Comissionamento e Testes de Aceitação

O aceite provisório do CPD, uma das responsabilidades principais do Integrador ou *General Contractor*, deve ocorrer durante a execução do projeto e das instalações do CPD, mediante a elaboração de um programa de aceite e procedimentos, cujo texto deve ser definido, no mínimo, 30 dias antes do comissionamento e submetido à operação e revisão do cliente. O Integrador deve fornecer 03 (três) cópias de todos os diagramas e documentos dos equipamentos instalados junto com os relatórios de testes, os manuais de operação e manutenção. O Comissionamento e Testes de Aceitação podem ser previstos e detalhados com subdivisões para os seguintes tópicos – Obras Cíveis; Energia; Aquecimento, Ventilação e Ar-condicionado; Sistemas de Segurança; Sistemas de Alarme e Monitoramento.⁴⁹

As verificações das Obras Civis devem enfatizar os aspectos dos sistemas prediais conforme conjunto básico exemplificativo de requisitos para as análises descritas a seguir : Controle dos Diagramas (verificar a conformidade com planos e especificações; verificar as premissas da área e do piso elevado); piso (verificar a conformidade com as especificações de piso nas áreas construídas; verificar a conformidade do piso elevado com as especificações do piso elevado; verificar o alinhamento e nivelamento do piso e do piso elevado; verificar os alinhamentos dos pedestais do piso elevado; verificar a limpeza do piso; inspecionar os recortes do piso elevado); Teto (verificar o aspecto e a conformidade com as especificações; verificar o material; verificar a altura do teto contra a altura do piso elevado e do piso); Paredes/ Pintura/ Portas (verificar a conformidade com as especificações; verificar a operação das portas, batentes e identificações; verificar a qualidade de todos os itens); Janelas (verificar a conformidade com as especificações; verificar se as proteções físicas e contra o sol estão instaladas; verificar a vedação e o fechamento das janelas); Iluminação (verificar aspectos gerais e visuais das luminárias; verificar a conformidade com as especificações da instalação de luminárias e ligação elétrica, dos interruptores e das áreas atendidas, do nível de iluminação a ser medido a 85 cm acima do piso); Tomadas elétricas e telefone (verificar a conformidade com as especificações e desenhos; verificar a conformidade dos cabos com o especificado).

As verificações de Energia devem enfatizar os aspectos dos sistemas prediais conforme conjunto básico exemplificativo de requisitos para as análises descritas a seguir : Transformadores (verificar a conformidade das instalações de média e baixa voltagem, particularmente examinar os ajustes/ parâmetros dos fusíveis e disjuntores); UPS/No-Break - Inspeção Visual (verificar a instalação das UPS's e baterias, como: acessibilidade para obter leituras, identificação com label das unidades; conferir os labels com as especificações; verificar as conexões de energia e controle; verificar as tolerâncias pré-programadas de frequência e voltagem) e Teste Funcional (testar a operação com a UPS submetida à carga total e também com o gerador; realizar testes de manobras das UPS's para by-pass estático e retorno/by-pass estático para by-pass de manutenção e retorno/ controle de toda instrumentação;

realizar verificação das monitorações e alarmes tanto no local como remotas, inclusive com o termostato para alarme em alta temperatura; realizar teste de descarga dos bancos de bateria para regulagem após três descargas dos bancos; registrar a temperatura ambiente da sala de baterias e verificar se há diferenças de temperatura significativas na sala; descarregar 100% a carga das baterias desligando, por exemplo, o banco 1 com o banco 2 permanecendo ligado, visando a verificação de autonomia das baterias e a integridade de todas as conexões; registrar a voltagem das baterias a cada dois minutos ou pelo menos duas vezes durante a descarga, sendo que todas as voltagens das células devem ter pelo menos 10% do total das células; verificar se a carga é transferida para o circuito de by-pass quando o fornecimento de energia das baterias é interrompido; descarregar 60% da carga das baterias desligando os bancos, observando as voltagens de descarga individuais das células; depois do desligamento automático das UPS's, reconectar os bancos e verificar o restart automático das UPS's; durante o ciclo de descarga e a cada 5 minutos registrar as tensões das células); Geradores - Inspeção Visual (realizar a verificação dos dados da placa de identificação contra as especificações; verificar a instalação dos vibradores e base dos geradores; verificar a tubulação de exaustão e silenciador; verificar a ventilação da sala na entrada/ saída, abafadores, ruído; verificar os tanques de abastecimento diários, principais bombas e tubulação de combustível; verificar o painel de controle, as conexões de controle e de energia, *bus-bar* ou *bus-way*) e Testes Funcionais (executar start-up automático na condição de desligamento de energia e desligamento automático no retorno da energia, registro dos tempos de demora para o start-up e desligamentos; realizar a operação das UPS's com pelo menos 60% da carga, controle de estabilidade operacional nos geradores e UPS's; executar a variação de frequência e tensão entre zero e carga total, sendo que a carga deve ser adicionada gradualmente; realizar a verificação do fornecimento de combustível automático do tanque diário; realizar duas horas de teste, se possível, com carga total, registrando-se as temperaturas do equipamento e da sala, além da corrente, tensão e frequência; executar o teste local e remoto completo dos alarmes e monitoramento; registrar nível de ruído dos geradores no exterior do prédio); Sistema de Distribuição de Energia – Inspeção Visual (Transformadores: verificar identifições, capacidade, proteção e os diagramas de distribuição; Painéis: verificar

instalação, conexões de energia e controle, ajuste/ parametrização de disjuntores, acessibilidade para manutenção e leituras; Cabos: verificação de bitola, instalação e bandejamento; Verificar a identificação dos painéis, instrumentos, disjuntores e cabos em conformidade com os diagramas; Verificar a instalação dos respectivos diagramas unifilares nas salas, de preferência em quadros protegidos por vidro) e Testes Funcionais (operar todos os disjuntores, verificar os funcionamentos dos instrumentos, relés, monitoramento local e remoto dos alarmes e sequência de fases; realizar o teste de carga de todos os painéis durante os testes de carga dos geradores e UPS's através da operação dos sistemas de climatização e das cargas das UPS's para as PDU's; executar os testes de operação manuais e automáticas das STS's); Aterramento - Inspeção Visual (realizar a verificação dos diagramas de aterramento; verificar o cabo de aterramento; verificar os cabos de distribuição de aterramento para os painéis de energia, UPS's e geradores) e Teste Funcional (verificar as medidas das impedâncias dos terras).⁵⁰

As verificações de Aquecimento, Ventilação e Ar-condicionado devem enfatizar os aspectos dos sistemas prediais conforme conjunto básico exemplificativo de requisitos para as análises descritas a seguir : Testes Gerais – Inspeção Visual (verificar a identificação do ar de entrada/ retorno; realizar a verificação dos locais de aberturas do ar de entrada/ retorno; certificar a eficiência da distribuição do ar; verificar que os difusores do ar frio não perturbam os ocupantes; verificar as proteções solares se houver; verificar se os difusores não estão muito próximos dos detectores de incêndio) e Inspeção Funcional (medir temperaturas e unidades das salas; medir o fluxo de ar em m^3/h ; medir o nível de ruído à um metro dos difusores); Sistema de Condensadores - Inspeção Visual (identificar calor nas tubulações de gás e água; verificar se as tubulações estão bem instaladas e isoladas e separadas; verificar a eficiência da distribuição do ar; verificar se o ar gelado vindo das unidades de ar condicionado não está causando desconforto aos ocupantes locais; verificar a proteção solar; verificar entrada de ar externo no sistema; verificar os condensadores e suas instalações) e Inspeção Funcional (medir a temperatura de Bulbo Seco da saída e do retorno do ar; medir a temperatura de Bulbo Seco da sala, verificando os graus em $^{\circ}\text{C}$ e a umidade relativa do ar em %; medir o fluxo de ar em

m³/h; medir o nível de ruído em DBA na distância de um metro dos difusores); Sistema de Ar na Sala de Computadores - Inspeção Visual (verificar as unidades de ar dentro do CPD e a eficiência da distribuição do ar; inspecionar o sistema de tubulação; verificar a equalização da distribuição abaixo do piso elevado; verificar áreas de fugas de ar no piso elevado e no forro; verificar as proteções solares nas janelas; identificar a renovação de ar do sistema; verificar os “status” e histórico de alarmes, temperatura em °C e umidade relativa do ar em % nas unidades de ar no CPD; observar vibrações mecânicas de medidas do Hígro Termógrafo) e Inspeção Funcional (medir a temperatura do ar gelado; medir temperatura em °C e umidade relativa do ar em % do CPD; medir o fluxo do ar de retorno; obter três leituras de velocidade do ar em m/h para o melhor caso, médio e pior caso; verificar possíveis obstáculos do retorno de ar para as unidades de ar do CPD, retirando-os quando possível; medir o fluxo da tomada externa para renovação do ar; medir o nível de ruído na distância de um metro da unidade de ar condicionado do CPD; medir o nível de ruído das unidades de condensadores a uma distância de cinco metros).

As verificações dos Sistemas de Segurança devem enfatizar os aspectos dos sistemas prediais conforme conjunto básico exemplificativo de requisitos para as análises descritas a seguir : Controle de Acesso e Detecção de Intrusão (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente todos os elementos, como leitoras de cartão, leitoras biométricas, etc; certificar que todas as partes de segurança de saída estão equipadas com barras de pânico ou equivalente); Detecção de Incêndio (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente toda a instalação; executar o teste funcional de cada detector; executar o teste funcional do sistema de detecção com as especificações e operação, por exemplo, se o alarme de duas zonas ou áreas suspende o funcionamento da climatização; verificar o funcionamento e operação dos alarmes locais e remotos); Extinção de Incêndio (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente toda a instalação; efetuar testes de simulação da desativação manual e automática do sistema incluindo os relés de alarme, de acordo com as especificações dos fabricantes; no caso de sistema de extinção por inundação de gás no ambiente;

verificar todos os extintores de incêndio, isto é, localização, sinalização, numeração e conformidade com os diagramas); Detecção de Líquidos e Vapores (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente toda a área de detecção e realizar pelo menos dois testes operacionais; verificar o funcionamento e operação dos alarmes e indicações remotas; se houver tubulações de gás ou água dentro da área verificar se as válvulas de desligamento funcionam, inclusive conforme as especificações e diagramas); Botões de Desligamento de Emergência (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente os botões protegidos por vidro e a sua localização; verificar os manuais de operação, os alarmes e monitorações remotas); Proteção Contra Descargas Elétricas e Atmosféricas (verificar a conformidade da instalação e operação com as especificações; verificar o aterramento dos cabos a terra; verificar que o sistema de aterramento e descargas estejam interconectados); Iluminação de Emergência (verificar a conformidade da instalação e operação com as especificações e diagramas; localizar uma verificação e testes funcionais).

As verificações do Sistema de Alarme e Monitoramento devem enfatizar os aspectos dos sistemas prediais conforme conjunto básico exemplificativo de requisitos para as análises descritas a seguir : Painel de Alarme e Monitoramento (verificar a conformidade da instalação e operação com as especificações; inspecionar visualmente a instalação dos painéis e elementos associados; certificar através de teste que todos os alarmes e status de controle funcionam em operação e integrados aos demais sistemas, local e remotamente); Outros Painéis (aplicar os mesmos testes que os do Painel de Alarme e Monitoramento).

O comissionamento do CPD constitui-se de um processo sistemático, que assegura que todos os sistemas estão trabalhando de modo correto e interativo com todos os demais, de acordo com o projeto, as especificações e as necessidades do negócio. Este objetivo pode ser alcançado desde o início da obra, ainda na fase de projeto, e durante a execução, aceite e garantia (para verificação da performance). O processo de comissionamento abrange e integra documentação, start-up de equipamentos, ajustes de sistemas de controle, teste de balanceamento, testes de *performance* e

treinamento. A constituição da Equipe de Comissionamento pode ser composta da seguinte forma : equipe técnica do cliente como primeiro interessado na qualidade final; empresa especialista em comissionamento; empresa responsável pela consultoria; empresa integradora; as empresas sub-contratadas para executar cada fase da construção, como obra civil, elétrica, mecânica, dentre outras. A contratação da Empresa Comissionadora deve ser efetuada diretamente pelo cliente da obra ou pela empresa de consultoria, sendo que a empresa Comissionadora deve dirigir e coordenar as atividades de comissionamento. Todos os membros da Equipe de Comissionamento trabalham em conjunto sendo cada um responsável pelas atividades contratadas originalmente. A empresa responsável pela Integração, ou General Contractor, em conjunto com a Empresa Certificadora devem estabelecer o PLANO DE COMISSIONAMENTO, cuja responsabilidade final deve ser da empresa Comissionadora, competindo a esta a integração de todas as atividades de Comissionamento.⁴⁹

As atividades típicas do Processo de Comissionamento ou Certificação podem ser descritas conforme segue : o comissionamento durante a construção começa com uma reunião sobre o escopo do projeto sendo conduzida pela Empresa Comissionadora, sendo que, nesta atividade o processo de comissionamento pode ser revisado com os membros da Equipe de Comissionamento/Certificação; outras reuniões podem ser necessárias durante as providências de melhorias do CPD para coordenar e planejar futuras atividades e resolver problemas; devem ser entregues a Empresa Comissionadora durante as atividades a documentação dos equipamentos, incluindo procedimentos detalhados de *start-up* (ativação); a Empresa Comissionadora deve trabalhar com a Empresa Integradora e as sub-contratadas na elaboração dos planos e documentação de *start-up*, inclusive elaborando para as empresas os *check lists* a serem realizados durante a fase de *start-up*; geralmente os controles e verificação de performance são iniciados ao nível de componente, para equipamento, para sistema, para integração de sistemas com *check-lists* sendo realizados e completados antes dos testes funcionais; as sub-contratadas e a Empresa Integradora devem executar e documentar todos os *check-lists* pré-funcionais, como também o *start-up* e o controle final, sendo que, a Empresa Comissionadora deve

documentar que as listas de controle e o *start-up* foram realizados de acordo com os planos aprovados e foram testemunhados pela mesma; a Empresa Comissionadora deve desenvolver procedimentos específicos de testes de equipamentos e de sistemas, sendo de competência das sub-contratadas e a Empresa Integradora a revisão dos procedimentos; os procedimentos são executados pelas sub-contratadas sob a direção e documentadas pela Empresa Comissionadora; problemas detectados durante os testes derivados de um material, instalação ou setup devem ser corrigidos e refeitos pelas sub-contratadas e sempre às suas custas; os procedimentos de testes Integrados de sistemas devem ser desenvolvidos pela Empresa Comissionadora e revistos pelos integrantes da Equipe de Comissionamento; os testes integrados de sistema devem ser executados pelas sub-contratadas e acompanhados pela Empresa Integradora e Empresa Comissionadora; a Empresa Comissionadora compete rever toda a documentação de operação e Manutenção; o comissionamento deve estar completo antes da conclusão final do projeto de melhorias ou construção do CPD; a Empresa Comissionadora deve rever, pré-aprovar e coordenar o treinamento a ser fornecido pelas sub-contratadas à empresa encarregada pela operação.⁴⁹

A abrangência dos Trabalhos da Empresa Comissionadora para o CPD, como uma construção de Missão Crítica, deve ser certificada de acordo com as *start-ups* dos fornecedores dos subsistemas principais. O comissionamento deve incluir as empresas instaladoras e os técnicos dos principais fornecedores, como: geradores, UPS's, climatização, controles, dentre outros. A performance dos sistemas e subsistemas será testada contra as especificações, e só então, os testes integrados de sistema serão realizados e sempre em conformidade com o projeto e suas especificações. Todos os testes devem ser gerenciados pela Empresa Comissionadora para a validação, portanto, de todo o adequado funcionamento do CPD. O Aceite Final consiste essencialmente na revisão de todos os trabalhos, que devem ser realizados dentro do período de garantia de um ano nos equipamentos e na avaliação de quaisquer problemas operacionais ocorridos neste período. O Aceite Final deve ser realizado pela Empresa Integradora e ser acompanhado pela Empresa Comissionadora. Embora o comissionamento apresente ao final um certificado do aceite de todo o projeto, recomenda-se que seja contratada empresa internacional com o objetivo exclusivo da certificação do CPD, nos moldes de certificação de

qualidade ISO, sendo possível também se obter uma certificação ambiental, cujo assunto passa a ser tratado no próximo tópico.

5.5 Certificação Ambiental (LEED)

Dentre as diversas certificações possíveis para se atestar a qualidade dos produtos e serviços aplicados ou as soluções desenvolvidas em um CPD, a mais recente e inovadora é a certificação ambiental oferecida pelo LEED-*Leadership in Energy and Enviromental Design*, cujos data centers também podem ser objeto de diferencial competitivo em alinhamento ao cenário atual de responsabilidade sócio-ambiental que abrange as Intituições Financeiras de Classe Mundial.

O movimento *Green Building* referiu-se ao desenvolvimento sustentável alguns anos atrás como sendo “a mais vibrante e poderosa força de impacto no seguimento de projeto e construção de edifícios há mais de uma década” e, desde então, nada aconteceu para diminuir a validade de seus efeitos sobre a indústria da construção civil, os quais não podem ser subestimados. O programa de certificação LEED-*Leadership in Energy and Enviromental Design* do USGBC-U.S. *Green Building Council* constitui-se de um sistema complexo de classificação “verde” para edifícios cujos projetos e construções possam contribuir para o desenvolvimento sustentável através do efetivo exercício de responsabilidade sócio-ambiental.⁵¹

O panorama geral do LEED em 2004 registrou as classificações de certificação em 04 (quatro) categorias distintas por tipo de espaço construído – *New Construction* (NC), *Existing Building* (EB), *Commercial Interiors* (CI) e *Core & Shell* (CS) – além de iniciar um projeto piloto na categoria *LEED for Home* (H), dentre os níveis sequenciais de pontuação considerados em 04 (quatro) patamares – *Certified*, *Silver*, *Gold* e *Platinum* - conforme demonstrado nas Tabelas 6 e 7 a seguir.⁵²

Tabela 6 – Pontuação Mínima dos Níveis LEED*Fonte : U.S. GREEN BUILDING COUNCIL*

Descrição	LEED-NC	LEED-EB	LEED-CI	LEED-CS
Certified (certificado)	26	32	21	24
Silver (prata)	33	40	27	30
Gold (ouro)	39	48	32	36
Platinum (platina)	52	64	42	48

Tabela 7 – Sistema de Pontuação do Programa LEED*Fonte : U.S. GREEN BUILDING COUNCIL*

Categoria do Crédito	LEED-NC	LEED-EB	LEED-CI	LEED-CS
Site Sustentável	14	14	7	15
Eficiência de água	5	5	2	5
Energia & Atmosfera	17	23	12	16
Materiais & Recursos	13	16	14	11
Qualidade do Ambiente Interno	15	22	17	13
Inovação e processo de desenho	5	-	5	5
Inovação em Up-grades, Operação e Manutenção	-	5	-	-
Total de Pontos Possíveis	69	85	57	65

O sucesso do desenvolvimento deste complexo sistema de classificação “verde” pode ser atribuído ao árduo trabalho em liderança dos respectivos comitês do *U.S. Green Building Council*, cujos resultados em 2004 contabilizaram 5.157 membros, 162 projetos certificados LEED e 1.614 projetos registrados, totalizando aproximadamente 18 milhões de metros quadrados de espaço construído, sendo que, além dos EUA, existem projetos LEED em mais de uma dúzia de países estrangeiros, incluindo a Índia, China e Brasil.⁵²

LEED for New Construction (LEED-NC)

O programa de classificação para edifícios “verde” LEED-*Leadership in Energy and Environmental Design* (Liderança em Projeto Ambiental e de Energia), conforme definição do *U.S. Green Building Council* (Conselho Americano para o Edifício Verde), pode ser descrito como sendo uma base consensual de âmbito nacional nos EUA, cujo sistema de diretrizes do mercado para classificação de edifícios foi desenhado para acelerar o desenvolvimento e implementação de práticas na edificação “verde”, em resumo, trata-se do primeiro sistema elaborado para o planejamento, construção e certificação dos melhores edifícios “verde” do mundo.

O programa LEED-*New Construction* (certificação para novas construções), ou simplesmente LEED-NC, funciona muito bem sobretudo por ser simples de entender e encontra-se dividido basicamente em 05 (cinco) categorias relacionadas ao site, conservação da água, energia, materiais, qualidade do ambiente interno, acrescentando-se ainda mais uma categoria para inovação e desenho. Cada categoria contém um número específico de créditos que possuem uma ou mais possibilidades de pontos. Um projeto que alcança a pontuação suficiente (26) pode obter a classificação “*Certified*” (certificado), subindo-se a pontuação (33) pode chegar ao nível “Silver” (prata), ou ainda, com maior pontuação (39) o nível “Gold” (ouro) até atingir o último nível (52 ou mais pontos) de classificação “Platinum” (platina), conforme demonstrativo que consta da Tabela 8 a seguir.⁵²

Tabela 8 – Níveis da Certificação LEED

Fonte : U.S. GREEN BUILDING COUNCIL

Classificação	Pontos Ganhos
Certified (certificado)	26-32
Silver (prata)	33-38
Gold (ouro)	39-51
Platinum (platina)	52-69

Eis o brilhantismo do programa LEED – simplicidade, estrutura competitiva e uma métrica de regras claramente estabelecidas com estratégias intrincadas que levam as equipes de gestão predial ao desafio de se equacionar uma questão complexa e multifacetada – conciliar o desenho sustentável e o desenvolvimento, assim, mais do que apenas seguir um check-list de critérios torna-se possível a implantação de edifícios plenamente integrados e bem desenhados.

LEED for Existing Buildings (LEED-EB)

A primeira coisa a ser salientada sobre o LEED-EB (certificação para edifícios existentes) trata-se uma análise do ciclo de vida útil do edifício na qual pode se verificar que 75% ou mais dos custos são gastos em operação e manutenção. Os prédios existentes (inclusive residências), uma vez consideradas as estatísticas a serem efetuadas em âmbito nacional, podem chegar a consumir perto de 40% da energia, adicionarem 40% da emissão atmosférica, consumirem 68% da eletricidade, 12% da água fresca e 88% da água potável, acrescentarem 40% dos dejetos sólidos municipais e usarem 40% de toda a madeira e materiais básicos da construção civil em mercados como nos EUA.⁵²

Outra coisa para se lembrar é que há muito mais prédios existentes de usos comerciais, industriais e institucionais (ex: perto de 100 vezes mais prédios existentes nos EUA) do que os que são construídos a cada ano. Teoricamente então, a certificação “green” em prédios existentes pode ter o dobro da ordem em tamanho e magnitude do impacto no consumo de energia e meio-ambiente do que pode ser alcançado com a certificação LEED para novas construções (LEED-NC). Eis a razão porque o LEED-EB tem crescido no enfoque dos aspectos de operação e manutenção dos edifícios (O&M), cuja atenção permanente pode contribuir para o alcance do pleno potencial destes, além de prover um caminho para recertificação dos edifícios que anteriormente alcançaram o LEED-NC ou até mesmo o LEED-EB que pode ser ampliado, visando produzir uma série de economias e benefícios potenciais no processo do gerenciamento de *Facilities*.

LEED for Commercial interiors (LEED-CI)

Este programa tem por objetivos a seleção de espaços alugados sustentáveis (Interiores Comerciais), o uso eficiente da água por inquilinos corporativos, a otimização do desempenho energético (especialmente a iluminação e seus controles), os materiais para os sistemas prediais no interior do edifício inclusos o mobiliário, carpete, pisos e a qualidade do ambiente interno. O LEED-CI também pode refletir um crescimento nos interesses que encorajam os inquilinos corporativos a selecionar espaços estabelecidos em comunidades que facilitem o acesso de pedestres (“walkable communities”) com pelo menos 10 a 20 serviços básicos disponíveis, tais como, bancos, lojas, escolas, correios, salão de estética, dentre outros.⁵²

LEED for Core & Shell (LEED-CS)

Este programa atende principalmente os investidores em escritórios de negócios, no varejo ou em prédios de uso misto, os quais são projetados para proprietários que não controlam o desenho de interiores e os acabamentos externos aplicados nos espaços construídos. O LEED-CS segue muito próximo dos requisitos aplicados pelo LEED-NC e a principal diferença consiste no processo de pré-certificação, sendo esta uma característica exclusiva do LEED-CS dentre todos os programas de certificação do LEED, cuja visão para o mercado permite tratar o projeto como se fosse certificado, mesmo antes do prédio ser construído. O processo de pré-certificação permite aos investidores obter uma aprovação prévia do USGBC-U.S. Green Building Council submetendo-se um plano de pontuação que o prédio deverá alcançar com base nos desenhos do projeto.⁵²

LEED for Homes (LEED-H)

O movimento do “Green Building” também chega em casa. Enquanto a essência dos programas LEED são direcionados ao mercado da construção não-residencial, o potencial do seguimento residencial não pode ser ignorado, pois representa 59% do total de investimentos na indústria da construção nos EUA. O programa LEED-H envolve um check-list de fatores relacionados ao uso da energia, gerenciamento da água, ambiente de trabalho, conservação da água e a qualidade do ambiente interno nas construções residenciais, cujos benefícios da certificação LEED-H permitem

uma diferenciação no mercado aos construtores deste seguimento, além da imagem pública positiva e o incremento de relações com as entidades oficiais do governo na localidade do empreendimento.⁵²

Em resumo, os programas de certificações LEED em suas diversas categorias sob a bandeira do Desenvolvimento Sustentável preconizada pelo movimento do “Green Building”, cujo crescimento e aplicação tem se evidenciado nos diversos seguimentos da indústria da construção civil em todo o mercado mundial, visam produzir os benefícios resultantes da responsabilidade sócio-ambiental aplicada ao desenho sustentável no projeto de edificações produtivas – incremento de produtividade no trabalho, crescimento da satisfação no exercício profissional e redução do absenteísmo, e por consequência, esse nível de consciência também se estende para as construções residenciais com o programa do *LEED for Homes* (LEED-H), cujo exame das condições de sustentabilidade aplicadas aos projetos, construções, operação & manutenção das edificações, pode contribuir significativamente com impactos positivos aos negócios de empresas e organizações, evidenciando as experiências em “*green building*” que cresceram apreciavelmente em 2004, conforme demonstrativos das Tabelas 9 e 10 a seguir.

Tabela 9 – Crescimento da Certificação LEED

Fonte : U.S. GREEN BUILDING COUNCIL (Outubro/2004)

Ano	Número de Projetos
1999	1.100
2000	8.400
2001	16.800
2002	80.000
2003	141.000
2004	194.000

Tabela 10 – Comparativo de Membros do USGBC

Fonte : U.S. GREEN BUILDING COUNCIL (Outubro/2004)

Descrição	Ano de 2003	Ano de 2004
Empresas Profissionais	2256	3385
Construtores Contratantes	410	675
Fabricantes de Produtos	244	392
Organizações s/ fins lucrativos	134	204
Universidades, Institutos de Pesquisa	96	167
Proprietários e Locadores	35	88
Agências Federais	25	21
Concessionárias	19	31
Corporações e Varejistas	22	27
Instituições Financeiras e de Seguros	3	6
Total	3.376	5.147

Os programas de certificação LEED dos EUA não são os únicos e nem os primeiros participantes no cenário mundial do movimento “green building”, pois a Europa vem pensando “verde” há muito tempo, desde que, nos anos 80 o governo do Reino Unido estabeleceu o BRE-*Building Research Establishment* visando promover a pesquisa relacionada aos edifícios que introduziu em 1990 o BREEAM-*Building Research Enviroment Assesment Method*, a primeira ferramenta de avaliação ambiental a ser utilizada internacionalmente que foi desenhada para análise de desempenho ambiental tanto de novas construções quanto de prédios existentes e que serve de base para programas equivalentes utilizados na Nova Zelândia, Austrália e Canadá. Outros países europeus, incluindo França, Alemanha, Suíça e Finlândia também desenvolveram esforços em projetos para se definir metodologias visando promover a sustentabilidade e aplicar análises do ciclo de vida em edifícios, resultando em ferramentas de avaliação como o software Eco-Quantum de Amsterdam, o Projeto Regener, a metodologia Eco-invent 2000 da Suíça, o programa Blue Angel da Alemanha e o programa Nordic Swan dos países europeus do Norte.⁵³

As emergentes organizações não-governamentais, WGBC-*World Green Building Council* e iiSBE-*International Initiative for a Sustainable Built Environment*, envolvendo cerca de 20 países incluindo Austrália, Canadá, Índia, Japão, Korea, Espanha e os EUA, encontram-se com ações no sentido de desenvolver um sistema de avaliação de desempenho ambiental intencionando produzir um padrão globalizado para facilitar a troca de informações entre países, bem como, desenvolver guias de práticas para a criação de *Green Building Councils* (Conselhos de Prédios Verdes) em outros países.

Os maiores bancos que compõem o cenário globalizado de financiamento aos projetos de infra-estrutura passaram a adotar voluntariamente alguns critérios mínimos de responsabilidade social e ambiental que devem ser atendidos para a concessão de crédito. O conjunto de regras chamado de “*Equator Principles*” (“Princípios do Equador”) foi desenvolvido pela IFC-*International Finance Corporation*, um braço financeiro do Banco Mundial, cujos critérios abordam o impacto ambiental do projeto sobre a flora e fauna, a exigência de compensações em dinheiro para populações afetadas, a proteção à comunidades indígenas e proibição de financiamento quando há uso de mão-de-obra infantil ou escrava, além de, classificar os empréstimos em três categorias com relação ao risco ambiental e social – “A” para a condição de alto risco, “B” para o risco médio e “C” quando há baixo risco. A base desta classificação utiliza-se de regras chamadas de “salvaguardas” que foram desenvolvidas pela IFC e devem ser aplicadas pelos bancos nos empréstimos acima de US\$ 50 milhões.¹²

Assim, considerando que ao adotar os “Princípios do Equador” os bancos comecem a aplicar sistematicamente os critérios de responsabilidade sócio-ambiental aos projetos de negócios financeiros corporativos, inevitavelmente, deverão também fazer o mesmo em outros aspectos de seus negócios no varejo e em suas próprias operações internas, cujo cenário aponta para o alcance de melhores resultados nos projetos, com reduções de custos enquanto sobretudo permitem promover a sustentabilidade.

Neste sentido, os programas de certificação LEED ou seus equivalentes disponíveis, podem contribuir efetivamente com as Instituições Financeiras de Classe Mundial inclusive na preparação para a Gestão Completa de Infra-estrutura e Instalações nos Ambientes de Missão Crítica em Tecnologia da Informação, constituindo uma base de apoio ao Desenvolvimento Sustentável, o qual não pode ser visto apenas como uma coisa boa de se fazer mas como um componente essencial do gerenciamento de riscos e melhoria dos controles internos que visam alavancar os negócios da Organização

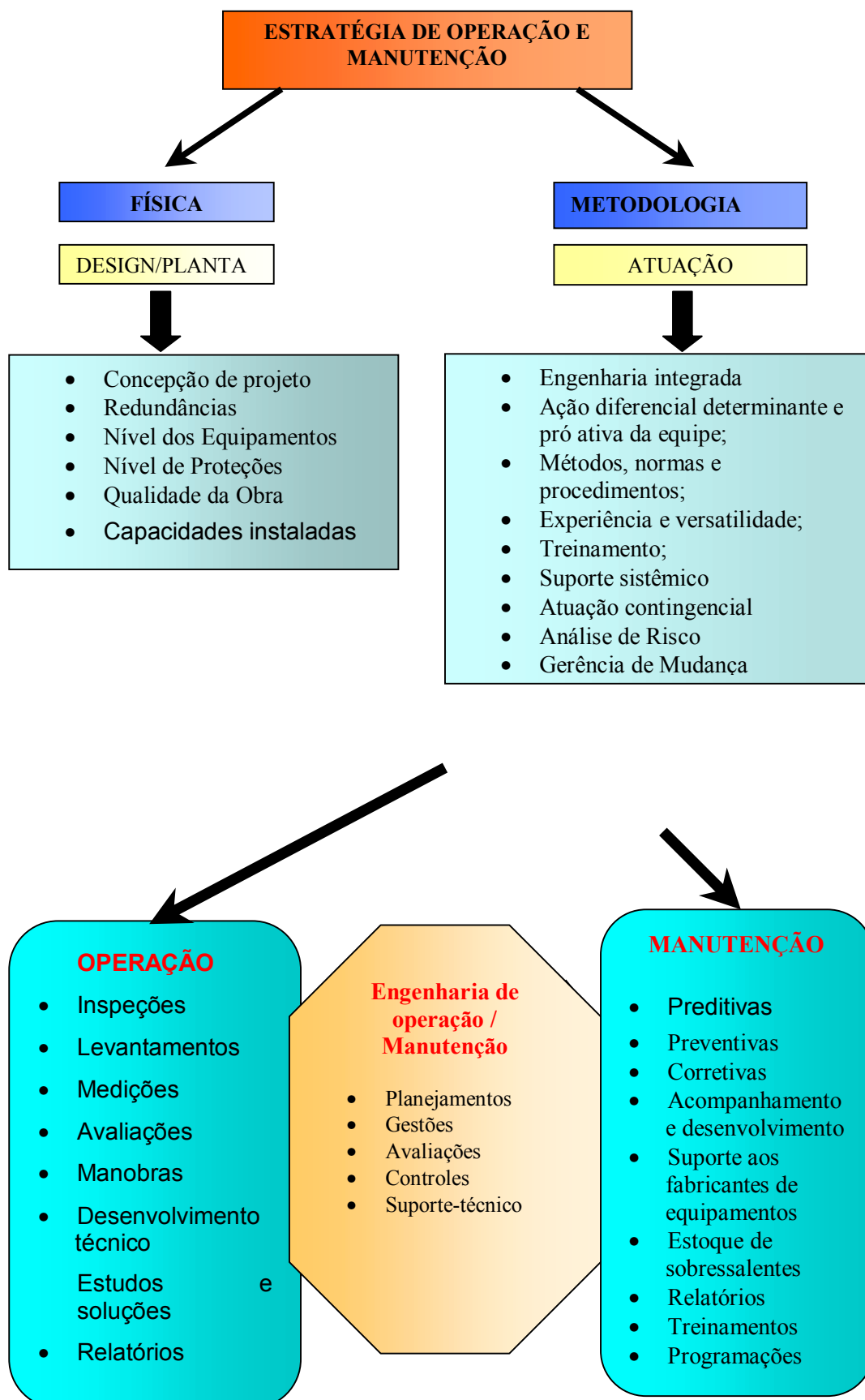
5.6 Operação e Manutenção do CPD

As construções de ambientes críticos evoluíram, como vimos, para atender clientes que necessitam de altíssima disponibilidade, confiabilidade 24 horas ao longo de todo o ciclo de vida do negócio. Assim, torna-se imprescindível, pois, a utilização de Metodologia nas áreas de Operação e Manutenção para garantir que o cliente possa se concentrar no seus negócios. Os Medidores que possam demonstrar esta qualidade devem ser implantados e gerenciados constantemente.

Neste tópico encontram-se os aspectos gerais e particulares a serem observados durante a operação e manutenção do CPD, entendendo-se como fundamental que a equipe responsável pela Operação e Manutenção esteja integrada desde a construção ou etapa inicial de melhorias do CPD, o mais cedo possível, tal como para a empresa responsável pela certificação. A Engenharia de Operações trata-se de área específica responsável por operar, manter, diagnosticar e avaliar as instalações e infra-estrutura do CPD, conforme demonstrado na Figura 26 a seguir.

Figura 27 – Diagrama Típico da Engenharia de Operações

Fonte : SISTENGE



Assim, podemos descrever a Engenharia de Operações, conforme segue.⁵⁴

- ◆ **Operação:** as atuações sobre os acionamentos do sistema de infra-estrutura de instalações (*facilities*) e seus equipamentos são parte da operação propriamente dita, devendo esta envolver toda a responsabilidade técnica de funcionamento deste sistema. Isto implica em amplo domínio de atuação sobre o projeto, obra e equipamentos, contando com a metodologia, técnica de engenharia e treinamentos por parte da área responsável. É responsabilidade da área de operações de facilities utilizar e preservar toda a documentação das instalações de infra-estrutura, como: diagramas, projetos e manuais de equipamentos. Trata-se de um trabalho de engenharia de operação, onde a técnica deverá sempre pautar todo o desenvolvimento técnico e acompanhamento das instalações, estudando e dando seguimento assistido aos recursos destas e antevendo soluções contingenciais, para preservação do nível de segurança operacional do CPD.
- ◆ **Assistência de Engenharia Permanente:** é efetuada pela equipe residente de engenharia de operação e deverá ser complementada quando necessário pelo departamento de engenharia da empresa encarregada pela Operação e Manutenção. O objetivo dessas atribuições é o de orientar soluções técnicas a fim de manter a continuidade operacional, promovendo melhorias racionais e de segurança física, condizentes com as instalações do projeto.
- ◆ **Gerenciamento Técnico de Engenharia:** os serviços técnicos de manutenção a serem realizados por terceiros (fabricantes), deverão ter a sua gestão através da equipe de manutenção. Caberão nessas atividades as avaliações técnicas para solicitação e recebimento dos serviços que se fizerem necessários.
- ◆ **Manutenção:** compreende a execução de procedimentos e cuidados para com as instalações e equipamentos conforme orientação dos fabricantes, aumentando a confiabilidade e vida útil. Preventiva: executada para manter os equipamentos em condições de operação através de inspeção cujo objetivo é detectar e prevenir possíveis falhas. Os sistemas recomendados neste caderno básico permitem que manutenções preventivas sejam realizadas sem afetar a disponibilidade do CPD; Corretiva: executada para recuperar um equipamento para condição de operação satisfatória, depois que o equipamento apresentou degradação ou parada em seu

funcionamento; Preditiva: executada em função dos dados de avaliação técnica de campo e inspeção e sendo detectadas de possíveis riscos antecipamos o programa de substituição de peças ou equipamentos. Contratos de Manutenção : é fundamental que a manutenção preferencialmente, seja prestada pelos fornecedores dos equipamentos. Recomendamos que nos contratos de manutenção sejam consideradas cláusulas específicas de penalidades baseados em ACORDOS DE NÍVEL DE SERVIÇO ou SLA (Service Level Agreement), com os itens abaixo: Nos contratos a serem celebrados com estas empresas, bem como com a empresa responsável pela Operação e Manutenção, é fundamental considerar os medidores de qualidade de: MTBF – Tempo médio entre falhas do sistema e MTTR – Tempo médio necessário para recuperar o sistema, desde a constatação do problema até o teste final. Para cada contrato devem ser estipuladas penalidades sempre que os medidores forem alcançados. São 3 (três) os elementos a serem negociados com as empresas fornecedoras: “Expertise” do corpo técnico; Tempo de atendimento à chamada; Disponibilidade de peças de exposição.

A operação de um site de missão crítica deve ser consistente e necessariamente apoiada em metodologia, que comprovadamente garanta as condições normais e críticas. É fundamental que um sistema de gestão e inteligência predial seja instalado e competentemente utilizado pela equipe responsável pela operação. A metodologia deve garantir que toda a documentação de engenharia, toda a documentação de equipamentos, todos os procedimentos críticos estejam sempre disponíveis, tais como : Manuais de operação/ manutenção de todos os sistemas como UPS, geradores, painéis de controle, detectores de fumaça, extintores de incêndio, etc; Conjunto completo de desenhos e diagramas; Diagrama unifilares de toda a distribuição de energia; Diagrama de blocos do sistema de climatização; Cópia de todos relatórios de testes dos fabricantes dos equipamentos; Cópia dos testes de aceite do CPD; Registro das leituras de operação; Procedimentos de operação de todos os equipamentos, subsistemas e sistemas; Procedimento para gerência de mudanças; Procedimentos para controle das manutenções.

A metodologia deve ainda abranger os tópicos que segue.⁵⁴

- ◆ **Plano de Teste de Sistema Crítico:** um plano de teste detalhado e documentado deverá ser desenvolvido para cada sistema, que apóia estas operações críticas. O plano simulará situações reais de perda e deverá ser testado com frequência específica, com cargas mais altas e mais baixas.
- ◆ **Operadores e Treinamento:** treinamentos documentados e planos de re-certificação devem estar sempre em regime para garantir, que o pessoal da operação tem conhecimento e experiência para operar o sistema e responder prontamente a seus alarmes.
- ◆ **Procedimentos de Ação em caso de Emergência:** procedimentos documentados para ações em caso de emergência devem estar definidos e implantados. Estes procedimentos definem ações, papéis e responsabilidades para responder a uma emergência. Os procedimentos devem incluir mecanismos de notificação de alarme, procedimentos de resposta, números a serem acionados em caso de emergência, procedimentos de escalonamento e procedimentos de desligamento de cargas. Deve estar prevista no projeto o acionamento automático de operadores e este implantado no Sistema de Automação Predial.
- ◆ **Capacidade Crítica da Infra-estrutura:** o pessoal operacional deverá medir e documentar periodicamente as cargas dos equipamentos e comparar estas medidas com os padrões estabelecidos no projeto. É importante que a equipe de operação possa ser engajada ao projeto em suas fases iniciais.
- ◆ **Plano de Manutenção Preventiva:** um plano documentado deve ser implantado para todos os equipamentos críticos instalados. O plano deve incluir todos os as-built e especificações, desenhos detalhados dos equipamentos, descrição dos projetos e manuais de operação e manutenção (O&M).
- ◆ **Procedimentos para Sala dos computadores:** procedimentos documentados devem ser desenvolvidos para estabelecer e manter os parâmetros de energia e refrigeração para cada sala específica de equipamentos que suportam a Tecnologia da Informação.

- ◆ **Atividades de Contratadas/Vendedor:** treinamento e procedimentos devem ser aplicados e desenvolvidos para garantir que as empresas contratadas e fabricantes estejam aptas a garantir os níveis exigidos de segurança e operação. Os operadores devem estar treinados para garantir e acompanhar estes procedimentos.
- ◆ **Manuais de Operação e de Manutenção:** um jogo completo de manuais de operação e manutenção deve ser preparado e estar na sala de operação e controle. Todos os sistemas, subsistemas, equipamentos e componentes devem estar documentados.
- ◆ **Inspecões do Site:** deve ser preparado um detalhado programa de inspeção das instalações para revisão e aprovação. Todo o pessoal de operação e manutenção executará uma inspeção total a cada troca de turno e elaborará um relatório completo de pontos a serem revisados.
- ◆ **Fabricante de Equipamento Original (OEM):** a manutenção e o serviço de todo equipamento ou sistema crítico deve ser executado, preferencialmente, pelo fabricante ou um autorizado do mesmo (não um terceiro). O suporte da engenharia do fabricante e seus engenheiros de campo devem ser contratados para os serviços programados ou emergenciais. Os as-built, toda documentação e desenhos necessários à manutenção dos sistemas e equipamentos deve ser mantido pelo fabricante e atualizados sempre que houver mudanças.
- ◆ **Gerenciamento de chamadas:** deve haver documentação e acompanhamento e registro das chamadas técnicas recebidas e feitas entre o cliente e terceiros provedores de serviço.
- ◆ **Relatórios de Serviço de campo:** relatórios detalhados com conclusão de todos os serviços de manutenção preventivos e emergenciais realizados.
- ◆ **Operação 24x365:** a operação deve monitorar cada sistema/componente crítico. Este monitoramento deve supervisionar alarmes em tempo real. Eventos não atendidos no tempo planejado devem ser reportados a um Centro de Operações para gerenciamento do problema e para os responsáveis da cadeia de escalonamento.

Capítulo 6 – GOVERNANÇA EM FACILIDADES PREDIAIS

Neste capítulo, como último ponto do presente trabalho trataremos os detalhes da proposta de um Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras, incluindo um plano básico de reestruturação para o Gerenciamento de Facilidades com uma visão estratégica e um conjunto de ações práticas visando estabelecer a Governança em *Facilities*.

Qual o cenário das empresas que experimentam um enorme crescimento de suas operações, fundamentadas em Tecnologia da Informação, e, neste contexto, também agravado por novas exigências de agências reguladoras do mercado, precisam de novos prédios e melhorias significativas nas demais instalações físicas de Missão Crítica, bem como no demonstrativo de controles internos do processo de Gestão de Infraestrutura e Instalações Prediais ? O pesadelo acontece como no adágio popular do ramo da construção - “Qualidade, Rapidez e Custos Moderados são essenciais, mas não se pode ter todos os três, portanto, escolha os dois mais importantes” – o grande desafio é o de se equacionar os resultados que os recursos de MCF-*Mission Critical Facilities* (Facilidades de Missão Crítica) devem entregar às áreas de “TI & Business” (suportar os requisitos imediatos de TI ou promover um planejamento estratégico de longo alcance e alinhado aos negócios da empresa?) e este é o caminho mais curto para os desentendimentos de clientes e prejuízos de reputação da Organização. Como resultado, o Gerenciamento de Facilidades deve amparar e proteger este negócio, no qual as empresas com aplicações de Missão Crítica encontram-se apoiadas por técnicas de Governança Corporativa que fizeram emergir a necessidade de um modelo de “Governança em TI”, e assim, também se faz necessário desenvolver um novo padrão de controles internos dos ativos físicos ora denominado de “Governança em *Facilities*”, onde o ‘know-how’ de TI, Legislações, Administração e “Expertises Multidisciplinares” do Gerenciamento de Facilidades, devem ser sobrepostos aos princípios tradicionais do desenho e modelo de atuação da engenharia e arquitetura.

Além das diretrizes de acionistas assertivos, competição agressiva e legislações/normativas emergentes, há muitas outras questões que ocupam o tempo do CEO-*Chief Enterprise Officer* e que afetam toda a estrutura de Governança Corporativa, de modo que, tanto as questões de TI quanto de MCF-*Mission Critical Facilities* são alvos freqüentes de pouco entendimento e, conseqüentemente, de menor prioridade, a despeito do crescente suporte destas áreas aos negócios da empresa. Portanto, em alinhamento às práticas da “Governança em TI”, como seria possível se estabelecer uma “Governança em *Facilities*” ? As empresas de sucesso podem entender os requisitos de “TI & *Facilities*” e explorar os benefícios associados à gestão de riscos operacionais, da seguinte forma :

- ✓ Alinhando o Gerenciamento de Facilidades (GF) com as estratégias de TI e de negócios da empresa;
- ✓ Difundindo as estratégias e objetivos de GF por toda a organização;
- ✓ Provendo estruturas adequadas para facilitar a implementação da estratégia e objetivos de GF (“*Facilities Management*”);
- ✓ Criando relacionamentos construtivos e comunicações efetivas entre os “Negócios, TI & GF”, bem como junto aos clientes e parceiros externos;
- ✓ Insistindo que um modelo para o controle interno do GF seja adotado e implementado;
- ✓ Mensurando e incrementando o desempenho do GF (“*Facilities Management*”);

Enquanto o desenvolvimento da “Governança Corporativa” tem sido essencialmente dirigida em busca de transparência e proteção do valor das ações da empresa, a complexidade e criticidade do Gerenciamento de Facilidades (“*Facilities Management*”), com ênfase ainda mais específica na Gestão de Facilidades de Missão Crítica em ambientes de TI, tem criado um degrau de dependência que chama por um foco na “Governança em *Facilities*” a ser estabelecida como um imperativo dos negócios atuais. A “Governança em *Facilities*” não é uma tarefa isolada e constitui-se parte integrante da “Governança em TI” e de todas as práticas de “Governança Corporativa”, sendo necessário integrar estas três partes com o

reconhecimento do Gerenciamento de Facilidades (“Facilities Management”) como também essencial e prioritário na empresa, ao invés de algo praticado em isolado e secundário, considerando a sua atuação como demonstrado a seguir na Figura 27. Não se pode prescindir que a atuação do Gerenciamento de Facilidades deve acompanhar toda a evolução do ciclo de vida da edificação, considerando desde a fase de concepção (escolha de local e projeto), bem como a construção, operação, manutenção, modernização, aquisição ou disposição, atribuindo uma visão holística de conhecimentos multidisciplinares que visa tornar o espaço construído plenamente apropriado às pessoas, equipamentos e funções de atividade-fim no suporte aos negócios da Organização.

Figura 28 – Descrição do Processo da Gestão de *Facilities*

Fonte : ARCHIBUS INC.



Certamente que, no exercício efetivo da “Governança em *Facilities*”, torna-se essencial incluir nas posições de Diretoria Executiva (“Board”) um adequado perfil profissional específico de GF, o qual permita elaborar as questões corretas e garantir que as respostas sejam perfeitamente entendidas, as ações precisas sejam formuladas

e os resultados sejam monitorados. Este cenário pode ser alcançado através da seguinte combinação de fatores :

- Criação do cargo de CFMO-*Chief of Facilities Management Officer* servindo o “Board” (Alta Direção Executiva), ao lado dos CIO-*Chief Information Officer* e do CFO-*Chief Finance Officer*, como providência apropriada às instituições com elevada dependência de TI e, conseqüentemente, também de MCF-*Mission Critical Facilities* (Facilidades de Missão Crítica);
- O membro do “board” (Alta Direção Executiva) cujo CFMO se reporta deve possuir um perfil apropriado aos negócios relacionados com TI e MCF-*Mission Critical Facilities*;
- Eleição de um Diretor Departamental de *Facilities* (não executivo), com o apropriado perfil profissional em Gerenciamento de Facilidades (“Facilities Management”);
- Participação indispensável do Diretor Departamental de *Facilities* em reuniões periódicas do Comitê Executivo de TI;
- Programa de educação formal aos membros do “board” (Alta Direção Executiva) aos negócios relacionados com o MCF-*Mission Critical Facilities* (Facilidades de Missão Crítica).

Não por mero acaso, ao se conceber um novo modelo de atuação da **Gestão de Facilities** que se proponha a ser capaz de realizar a “Gestão Completa de Infra-estrutura e Instalações” e oferecer um efetivo controle de informações dos ativos físicos da empresa, o **planejamento estratégico** deve considerar um ambiente visionário de atuação, cuja **primeira onda** de implantação deve centrar-se no atendimento aos Departamentos de Informática (órgãos vitais da empresa), a **segunda onda**, utilizando-se do aprendizado anterior, pode se estender aos demais elementos do corpo da empresa e, por último mas não menos importante, a **terceira onda** pode ser o grande alvo de atuação da **Gestão de Facilities** em Instituições Financeiras de Classe Mundial, na qualidade de um novo segmento de “*business*” no setor bancário, ou seja, a criação do **Bank Facility** como uma ferramenta de venda do conhecimento adquirido na gestão dos próprios ativos físicos e um canal de escoamento deste novo produto, além dos diversos outros produtos específicos

existentes no setor, tornando ainda mais efetiva a participação do **Gerenciamento de Facilidades como Alavanca de Negócios no Setor Bancário**.

O presente trabalho, objeto também de seu próprio planejamento estratégico, pretende ater-se somente à primeira onda do planejamento de **Gestão de Facilities** para Instituição Financeira de Classe Mundial, visando atender ao requisito de dissertação para a conclusão do curso de MBA/Gerenciamento de Facilidades da Universidade de São Paulo. A segunda onda, com enfoque na modelagem de um sistema detalhado de **“Governança em Facilities”**, pode ser alvo de um plano de pesquisa para mestrado e a terceira onda, com enfoque num plano de negócios para viabilizar a idéia de **Bank Facility**, pode ainda ser a base de um plano de pesquisa para doutorado no Gerenciamento de Facilidades para Instituições Financeiras de Classe Mundial, haja visto o tamanho do desafio, abrangência e complexidade do contexto de atuação deste tipo de organização, cuja função transcende o universo econômico, envolvendo também a esfera da responsabilidade sócio-ambiental, significando ser capaz de **atender à mais completa gama de necessidades e públicos do mercado**, ou seja, **ser um banco completo**, capaz de ajudar a vida de seus clientes a ser também mais completa.

O conceito **“completo”** é muito simples em sua forma, e, exatamente pela força de síntese que só as coisas simples e simbólicas possuem, ele é capaz de expressar de forma abrangente toda a nossa proposta para a “Gestão Completa de Infra-estrutura e Instalações” expressa na atuação da **Gestão de Facilities**, com base numa visão do **“Gerenciamento de Facilidades como Alavanca de Negócios no Setor Bancário”**, a ser concebido com base no lançamento de uma proposta de **Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação em Instituições Financeiras**.

Portanto, a proposta de um Modelo de Governança em *Facilities* encontra-se centrada na visão de que **o controle efetivo das informações sobre os ativos físicos de uma empresa, constitui-se fator crítico de sucesso no desenvolvimento de ações para o efetivo Gerenciamento de Facilidades, com o propósito de atender**

as exigências do cenário atual no setor bancário, pois os requisitos neste mercado, apontam para a necessidade de uma estrutura autônoma com atuação no âmbito estratégico de negócios, contando com soluções integradas na automatização das ferramentas de apoio à gestão especializada e que possam gerar segurança através da Gestão Completa de Infra-estrutura e Instalações das Organizações, ou seja, através de um modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação em Instituições Financeiras de Classe Mundial.

Assim, o Gerenciamento de Facilidades Prediais do setor bancário tem a necessidade de uma **estrutura autônoma com atuação no âmbito estratégico de negócios, contando com soluções integradas na automatização das ferramentas de apoio à gestão especializada**, cujos recursos podem ser alvo de uma defesa sólida na abordagem de no mínimo 10 (dez) razões que podem justificar o argumento, conforme segue :⁵⁵

- 1) **Reduzir o Custo Total de Propriedade** – o imperativo de contenção das despesas com infra-estrutura e instalações existentes pode ser alcançado ao se prolongar a vida útil dos ativos com uma melhor manutenção preventiva, maximizando-se os investimentos com um acompanhamento confiável da posse, utilização, condição física, localização, desempenho e várias outras informações gerenciáveis sobre pessoas, processos e propriedades;
- 2) **Minimizar os Investimentos Desnecessários** – com um inventário preciso pode-se evitar a compra ou locação desnecessárias de novos espaços, equipamentos ou outros ativos físicos, permitindo-se economizar recursos realocando ativos ao invés de adquirir novos;
- 3) **Controlar e Gerir os Ativos de modo eficaz** – não se pode gerenciar o que não se controla; torna-se necessário ter acesso imediato aos detalhes da utilização dos espaços, ativos, propriedades, estatísticas dos equipamentos, inventários de bens, inspeções de condições físicas, relatórios gerenciais, planos de manutenções, e outras informações em tempo real que permitam alocar recursos de acordo com as necessidades da organização;

- 4) **Aumentar a Eficiência Operacional** – economia de tempo ao agregar valor ao trabalho de todos aproveitando a informação existente ao invés de reconstruí-la; a implantação de um repositório centralizado com toda a informação da infra-estrutura e instalações evita redundâncias, melhora a consistência e proporciona a exatidão dos dados sobre os ativos físicos;
- 5) **Facilitar a Tomada de Decisões Estratégicas** - o fato de dispor de toda a informação de infra-estrutura e instalações em um único local, facilita a avaliação do portfólio de ativos assim como a previsão de necessidades futuras;
- 6) **Compartilhar facilmente a informação através de toda a organização** – acesso facilitado aos dados de diversas aplicações, sistemas e locais, compartilhando de forma transparente a informação com outros departamentos da organização, incluindo-se os sites remotos;
- 7) **Aumentar a produtividade do pessoal** – a eliminação virtual da tarefa improdutiva de se manter várias bases de dados pode reduzir o esforço empregado na realização das tarefas cotidianas, ainda que necessárias, reduzindo também a energia e os recursos de pessoal;
- 8) **Produzir rapidamente relatórios gerenciais confiáveis** – as solicitações de informações podem ser satisfeitas em questão de segundos, tanto internas quanto externas, em formato padrão de apresentação com excelência na composição automatizada de dados; a ligação dos desenhos com uma base de dados pode oferecer facilmente a informação sobre espaços, ativos e pessoal, em cumprimento de legislações específicas que assim requerem a disponibilidade destas em inspeções regulares;
- 9) **Visualizar a imagem gráfica dos ativos** – a atualização simultânea e bidirecional entre desenhos e bases de dados acelera o fluxo da informação de forma gráfica e precisa através da corporação;
- 10) **Melhorar a visibilidade na organização** – um verdadeiro processo coordenado de Gerenciamento de Facilidades Prediais somente pode ser alcançado ao se compartilhar de forma automatizada toda a informação inerente à gestão da infra-estrutura e instalações da organização, junto aos

demais departamentos incluindo Finanças, Tecnologia da Informação, Recursos Humanos, Patrimônio e outros gestores envolvidos;

A área responsável por sistemas de Facilidades Prediais de Missão Crítica em Instituições Financeiras de Classe Mundial, encontra neste cenário um conjunto de condições favoráveis ao lançamento de um **Plano Básico de Reestruturação**, visando a atualização do modelo existente e alinhamento às mais recentes boas práticas do mercado, desta forma, sendo capaz de estabelecer um contexto facilitador ao crescimento e desenvolvimento pleno do potencial que tem, como elemento fundamental e crucial no suporte das funções estratégicas de Tecnologia da Informação (TI), responsável por alavancar a vantagem competitiva e negócios da Organização.

A efetivação de um **Plano Básico de Reestruturação** que permita estabelecer o posicionamento pró-ativo da **Gestão de *Facilities*** e a negociação de seu planejamento estratégico, inicialmente junto às áreas de Tecnologia da Informação (TI) visando contribuir para a garantia de segurança operacional através da “**Governança em *Facilities***” e, posteriormente, na efetividade do suporte aos demais elos de “**Governança em TI**” e “**Governança Corporativa**”, de tal maneira que seja preconizada a implantação de um **Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação em Instituições Financeiras de Classe Mundial**, pode ser concebido conforme as considerações dos tópicos que seguem.

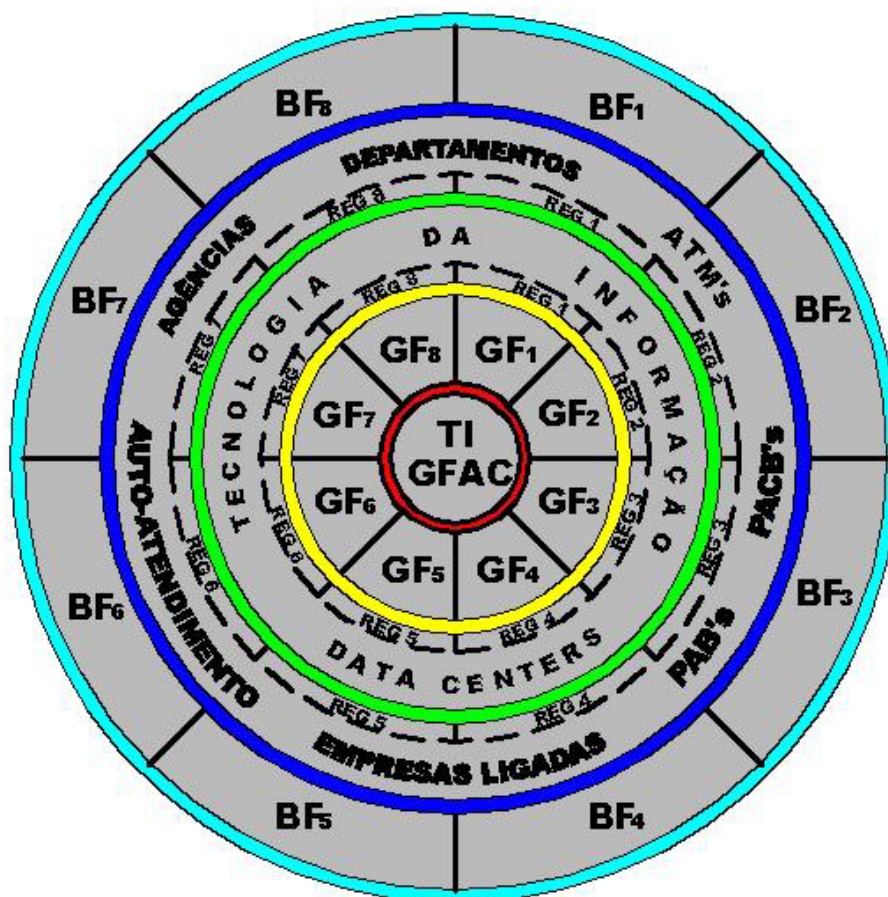
6.1 Proposta de Modelo Básico de Governança em *Facilities*

A proposta de um Modelo Básico de Governança em *Facilities* que parte da visão de uma estrutura organizacional autônoma com elevado nível de automatização e

especialização em processos, pode ser melhor definida a partir do entendimento da Figura 28 a seguir.

Figura 29 – Idéia Básica de Governança em *Facilities*

Fonte : AUTOR



Assim concebida a idéia da Governança em *Facilities*, temos ao centro a estrutura organizacional do TI-GFAC, ou seja, a área de Gerenciamento de Facilidades de Missão Crítica para TI com todos os seus recursos físicos e humanos. O primeiro elo indicado na cor vermelha representa os controles porporcionados pelo conjunto de ferramentas de apoio automatizado, sistemas de informações gerenciais, metodologias, boas práticas, normas e regulamentos, políticas de segurança e todas as ações que possibilitem efetivamente controlar e dirigir os resultados esperados dos ativos físicos na Gestão Completa de Infra-estrutura e Instalações de Facilidades de

Missão Crítica para TI, essencialmente sob os controles de um sistema que ora denominamos de *CAFG-Computer Aided Facilities Governance* (ex: produto ApertureVista400 das empresas Aperture Technologies, Inc./SPARKEL Soluções em Tecnologia). O segundo elo indicado na cor amarela representa os controles proporcionados pelo conjunto de ferramentas de apoio automatizado, sistemas de informações gerenciais, metodologias, boas práticas, normas e regulamentos, políticas de segurança e todas as ações que possibilitem efetivamente controlar e dirigir os resultados esperados dos recursos terceirizados aplicados por Gerenciadores de Facilidades (GF's) constituídos por empresas especializadas em *MCFM-Mission Critical Facilities Management* (Gerenciamento de Facilidades de Missão Crítica), essencialmente integrados aos sistemas do cliente e que possibilitam estabelecer a Governança em *Facilities*, sob os controles de um sistema que ora denominamos de *CAFS-Computer Aided Facilities Suppliers* (ex: produto Foconet da empresa FOCO Gerenciamento de Serviços). O terceiro elo indicado na cor verde representa os controles proporcionados pelo conjunto de ferramentas de apoio automatizado, sistemas de informações gerenciais, metodologias, boas práticas, normas e regulamentos, políticas de segurança e todas as ações que permitam efetivamente controlar e dirigir os resultados esperados dos ativos de TI & Telecom na Gestão dos Serviços de TI, essencialmente sob os controles de sistemas que visam estabelecer a Governança em TI como o denominado de *ITSM-Information Technology Service Management* (ex: produto Remedy IT Service Management para Gestão de Serviços em TI das empresas BMCRemedy/CSC Brasil) . O quarto elo indicado na cor azul escuro representa os controles proporcionados pelo conjunto de ferramentas de apoio automatizado, sistemas de informações gerenciais, metodologias, boas práticas, normas e regulamentos, políticas de segurança e todas as ações que possibilitem efetivamente controlar e dirigir os resultados esperados de todos os demais ativos físicos da Organização na visão da Gestão Completa de Infra-estrutura e Instalações, essencialmente sob os controles de um sistema denominado de *CAFM-Computer Aided Facilities Management* (ex: produto Archibus/FM-Enterprise das empresas ARCHIBUS, Inc./Grapho Design Software). O último elo na cor azul claro representa os controles proporcionados pelo conjunto de ferramentas de apoio automatizado, sistemas de informações gerenciais,

metodologias, boas práticas, normas e regulamentos, políticas de segurança e todas as ações que possibilitem efetivamente controlar e dirigir os resultados esperados de todos os ativos físicos de clientes da Instituição Financeira de Classe Mundial, na visão de criação de um novo segmento de negócios que ora denominamos de “*Business Facility*” (BF’s) ou ainda como “*Bank Facility*”, essencialmente sob os controles do conjunto de sistemas citados para os elos anteriores (CAFG/CAFS/ITSM/CAFM). Assim concebido, temos um modelo completo de Governança em *Facilities* tanto da própria Organização quanto para os seus clientes em potencial neste âmbito de negócios.

6.2 Ferramentas de Apoio Automatizado (CAFG/CAFM)

Como já vimos, o controle efetivo das informações sobre os ativos físicos de uma empresa constitui-se fator crítico de sucesso no desenvolvimento do Gerenciamento de Facilidades, com o propósito de atender as exigências do cenário atual no setor bancário, portanto, deve contar com uma estrutura organizacional autônoma de atuação no âmbito estratégico de negócios e com soluções integradas na automatização das ferramentas de apoio à gestão especializada. O contexto de “Governança Corporativa” dos negócios em Instituições Financeiras de Classe Mundial encontra-se apoiado em Tecnologia da Informação e ao enfrentar o desafio de se estabelecer a “Governança em TI” nasce o novo paradigma de se implantar um modelo para a “Governança em *Facilities*” da Organização.

Assim, se faz oportuno conceber a Gestão de *Facilities* para TI (TI-GFAC) que se proponha a ser capaz de realizar a “Gestão Completa de Infra-estrutura e Instalações”, oferecendo um efetivo controle de informações dos ativos físicos da empresa e contando com gestores especializados (GF’s), cujo planejamento estratégico pode considerar três ondas de implantação – Departamentos de

Informática (Tecnologia da Informação-Data Centers), Unidades de Negócios & Demais Gestores (Agências, Auto-atendimento, Departamentos, ATM's, PACB's, PAB's e Empresas Ligadas) e o Mercado de *Business Facilities* (BF's), além de objetivar o atendimento da mais completa gama de necessidades internas e de públicos deste segmento do mercado, contando com uma estrutura física de apoio que deve incluir uma central de monitoração de todos os ativos físicos da Organização, também denominado de FCC-*Facilities Comand Center*, o qual constitui-se um recurso essencial ao Modelo de Governança em *Facilities* ora idealizado, conforme o ilustrativo que consta da Figura 30 a seguir.

Figura 30 – Exemplo de *Facilities Comand Center*

Fonte : ELLERBE BECKET



A idéia do Gerenciamento de Facilidades ou “Facilities Management” como atividade multidisciplinar em benefício das edificações produtivas em ambientes de Missão Crítica para TI, a partir de um novo modelo de estrutura organizacional que considere o contexto regulatório e normativo do setor bancário nacional e as exigências do cenário para as Instituições Financeiras de Classe Mundial, não pode prescindir da Tecnologia da Informação nem mesmo para o próprio funcionamento, cujos controles automatizados do processo na “Gestão Completa de Infra-estrutura e Instalações” deve ser moldado com a utilização de ferramentas de apoio denominadas de CAFM-*Computer Aided Facilities Management* ou ainda com o enfoque de CAFG-*Computer Aided Facilities Governance*, nomenclatura que ora se

cria para denominar as ferramentas de controles específicos na Gestão de *Facilities* de Missão Crítica para TI, as quais se integram às demais ferramentas de apoio ao Gerenciamento de Facilidades Prediais da Organização.

O volume de informações necessárias para o correto desempenho do Gerenciamento de Facilidades é considerável, logo, gerenciar esta complexidade e a maneira como os dados são estruturados, coletados, ordenados, apresentados e atualizados, determina a utilidade e conveniência para sua utilização como suporte ao processo decisório. A própria informação também é um ativo da organização e como tal deve ser gerenciada, observando-se para ela os mesmos conceitos de qualidade, valores e riscos. A utilização de ferramenta de apoio automatizado na Gestão de *Facilities* como o CAFM, se bem empregada, tem o potencial de criar novas maneiras de desempenhar as atividades, agregando valor ao processo produtivo no suporte de funções gerenciais. A execução automatizada destas funções pode ser alcançada através do gerenciamento de informações relativas a quatro categorias:⁵⁵

- ◆ **Recursos Físicos** : locais, infra-estruturas, edifícios e seus ativos;
- ◆ **Serviços de Suporte** : administração, manutenção de propriedades, segurança, saúde, alimentação, limpeza, controle de frotas e de contratos;
- ◆ **Recursos Humanos** : gerenciamento de pessoal, contratos, recrutamento e treinamento;
- ◆ **Informações de Negócios** : processos, custos, contratos e políticas.

O Gerenciamento de Facilidades em Ambientes de Missão Crítica para TI, no contexto de elevadas exigências regulatórias para o efetivo demonstrativo de controles internos (ITIL, COBIT, COSO, ISO, SOX, BASILÉIA II, ABNT e outros), requer ainda maiores controles automatizados cuja ferramenta de apoio ora denominada de CAFG deve proporcionar o atendimento de aspectos específicos como os relacionados a seguir :⁵⁶

- Suportar os padrões e definições do ITIL para o gerenciamento de serviços e processos de estruturação da área de operações do Data Center, oferecendo uma solução integrada para gerenciar e automatizar os processos de Gerência de Configuração e Mudanças relacionados à infra-estrutura física do CPD;

- Localizar qualquer equipamento do CPD por número de inventário, número de série, endereço IP ou qualquer outro critério e atributo, visando a redução do MTTR-*Mean Time to Repair* mediante a visualização em planta ou em rack's;
- Indicar os equipamentos e aplicações críticas de TI afetadas por eventuais falhas ocorridas em disjuntores e PDU-*Power Distribution Unit*;
- Gerar relatórios que simplifiquem o gerenciamento da utilização e da capacidade dos recursos de infra-estrutura física do CPD;
- Priorizar e gerenciar a disponibilidade e continuidade dos serviços no CPD, bem como o esforço de recuperação em caso de alguma interrupção através de telas gráficas que identifiquem e classifiquem os níveis de criticidade dos equipamentos de TI na distribuição de lay-out do Data Center;
- Emitir alertas e condições de limites permitindo gerenciar os SLA-*Service Level Agreement* através do monitoramento dos principais indicadores de desempenho da infra-estrutura física do CPD;
- Controlar o acesso de técnicos em processos de serviços no CPD, mediante a liberação somente dos executantes com ordens de serviços aprovadas;
- Gerenciar os contratos de manutenção dos equipamentos e instalações do CPD, mediante o registro do histórico de intervenções, a visualização dos ativos físicos sem contrato em telas gráficas coloridas para a representação do lay-out e a emissão de relatórios por dados do contrato;
- Armazenar o histórico de todos os pedidos e detalhes para análises de mudanças e registro de desempenho para os SLA's;
- Gerenciar as conectividades de redes de comunicação de dados do CPD, mediante a documentação e emissão de relatórios de configurações;
- Permitir a integração com outras ferramentas de Gerenciamento em Ambientes de TI (Gerência de Redes, Gerência de Mudanças e Configurações, CAFM, CMMS, GED, BMS e outros).

6.3 Plano de Reestruturação da Infra-estrutura

A proposta de um Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras de Classe Mundial, além de contar com as ferramentas de apoio automatizado (CAFG/CAFM) também inclui a visão de uma estrutura organizacional autônoma como já vimos nos tópicos anteriores, portanto, em uma análise prática de planejamento do Gerenciamento de Facilidades para Missão Crítica podemos nos deparar com a necessidade de elaboração de um plano de Reestruturação da Infra-estrutura existente, cujos requisitos mínimos apresentamos no plano referencial exposto a seguir.

6.3.1 Objetivos

Desenvolver em linhas gerais as diretrizes para atualização da estrutura técnica e administrativa da área de Infra-estrutura Básica e Instalações para TI, visando estabelecer um alinhamento às mais recentes boas práticas do mercado e posicionar este seguimento de modo que todos possam entender claramente aquela que é a sua missão maior em Instituição Financeira de Classe Mundial, ser capaz de garantir a máxima segurança operacional dos ativos físicos nos espaços construídos destinados para abrigar e suportar os equipamentos e funções críticas dos Departamentos de Informática.

Estabelecer um novo posicionamento moderno, humano e multifuncional nos cuidados para o atendimento completo das necessidades expressas na crescente demanda por elevação dos níveis de conforto das pessoas e de máxima confiabilidade no ambiente físico de trabalho para TI.

Refletir todos os fatores críticos de sucesso para a “Gestão Completa de Infra-estrutura e Instalações”, em busca de inovações, produtos e serviços que possibilitem o constante trabalho de crescimento e desenvolvimento pleno do potencial que tem, como área de Missão Crítica para o suporte das funções estratégicas de Tecnologia da Informação (TI), responsável por alavancar a vantagem competitiva e negócios da Organização.

O objetivo maior deste Plano Básico de Reestruturação da Área de Infra-estrutura e Instalações para TI é o de contribuir efetivamente para a Instituição Financeira de Classe Mundial estar entre as primeiras do mercado, portanto, significa ter a mais completa gama de sistemas em infra-estrutura básica de instalações físicas de Missão Crítica para TI, bem como maior eficácia no controle de informações de seus ativos de facilidades prediais.

6.3.2 Sumário Executivo

O conjunto básico de diretrizes para a reestruturação técnica e administrativa da Área de Infra-estrutura Básica e Instalações para Tecnologia da Informação (TI), compõe-se de 05 (cinco) ações preliminares, a serem detalhadas e complementadas oportunamente, ora propostas conforme descrito a seguir :

- ☐ Estabelecer um novo nome para a área, a ser denominada de TI-Gestão de *Facilities*, ou simplesmente de TI-GFAC;
- ☐ Oferecer uma nova descrição de “Missão e Foco” e “Visão de Futuro” da Área de Infra-estrutura ora denominada conforme o tópico anterior;

- ❑ Apresentar um “Redesenho do Organograma da Área de Infra-estrutura, contendo a distribuição de responsabilidades em níveis estratégico, tático e operacional, de forma clara e transparente para a nova realidade do TI-GFAC;
- ❑ Definir um “Conjunto de Premissas Básicas do TI-GFAC que permita uma atuação coerente com o nível crescente de exigências estabelecido por agências reguladoras, legislações específicas, auditorias internas/externas, acordos de mercado, entidades de classes, políticas e códigos de ética, em âmbitos nacionais e internacionais;
- ❑ Propor um “Plano de Cargos e Funções” de acordo com o novo organograma da área TI-GFAC, contendo o descritivo de todos os cargos, perfil de profissionais e funções requeridas, visando contribuir e servir de base para o desenvolvimento posterior de um “Plano de Carreira, Salários e Treinamento” neste segmento;

6.3.3 Nova Denominação da Área

O “Gerenciamento de *Facilities*” é uma atividade relativamente recente, de nível superior, envolvendo campos da engenharia, arquitetura, administração, direito, TI e outros campos multidisciplinares do conhecimento, *com o objetivo de otimizar de forma abrangente tanto a utilização de recursos quanto a funcionalidade do edifício e seus sistemas, de maneira a torná-los instrumentos de alavancagem das atividades desenvolvidas em edificações produtivas*, como bem nos ensina os professores Dr. Moacyr Eduardo Alves da Graça e MSc. Paulo Eduardo Antonioli no Boletim Técnico BT/PCC/358 do Departamento de Engenharia da Construção Civil da Escola

Politécnica de Engenharia da Universidade de São Paulo-USP (sugestão : anexar cópia ao plano de reestruturação proposto).

Como consequência do avanço tecnológico, verificado sobretudo na última década do século XX, o uso do espaço construído, principalmente em aplicações de Missão Crítica para TI, alterou-se significativamente pela aplicação de tecnologia de eletrônica embarcada, demanda crescente por elevação dos níveis de confiabilidade, disponibilidade e flexibilidade da infra-estrutura básica de instalações físicas, bem como, pelo efetivo controle das informações dos ativos físicos e dos cuidados de necessidades específicas das pessoas e do ambiente de trabalho, num contexto de responsabilidade sócio-ambiental e de gestão dos riscos operacionais.

Em alinhamento às iniciativas do mercado, divulgadas por mídias específicas (revistas INFRA, CORPORATE, FACILITY e outras), além de associações, institutos, entidades de classe e o meio acadêmico (ABRAFAC, IFMA, BIFM, MBA/USP-GF, dentre outros), vimos através do presente documento sugerir a nova denominação da Área de Infra-estrutura como sendo TI-Gestão de *Facilities*, ou simplesmente TI-GFAC.

6.3.4 Descrição de “Missão” e “Visão”

O conjunto de recursos humanos e físicos, a serem destinados ao **TI-Gestão de *Facilities*** ou **TI-GFAC** conforme Planejamento Estratégico a ser desenvolvido oportunamente, têm por objetivo maior o de atender a **“Missão e Foco”** e **“Visão de Futuro”** oferecidas em novas descrições, conforme segue :

Missão e Foco

“Prover o Gerenciamento de *Facilities* de Missão Crítica aos Departamentos de Informática, visando contribuir na busca por um máximo funcionamento ininterrupto dos equipamentos e funções estratégicas de Tecnologia da Informação (TI), através do efetivo controle de ativos físicos da infra-estrutura básica de instalações prediais – elétrica, climatização e segurança física”.

Visão de Futuro

“O TI-GFAC como referencial de excelência da comunidade dos Departamentos de Informática (Processamento e Comunicação de Dados / Desenvolvimento de sistemas / Serviços Centralizados / Tecnologia do Negócio / Pesquisa de Informática) na “Gestão Completa de Infra-estrutura e Instalações”, reconhecido pelo seu contínuo e sólido crescimento na capacidade de responder com efetividade aos desafios propostos pela Organização, plenamente integrado e comprometido com as demandas estratégicas de Tecnologia da Informação (TI) e no cuidado permanente das necessidades para o conforto das pessoas no ambiente de trabalho”.

6.3.5 Redesenho de Organograma

O contexto de atuação proposto para a nova estrutura do **TI-Gestão de *Facilities***, ou simplesmente **TI-GFAC**, requer um redesenho das posições de trabalho, alinhado ao tamanho do desafio envolvido e às boas práticas de mercado, conforme hierarquia básica descrita a seguir :

Nível Estratégico de TI

- ♦ **Diretoria Executiva** – responsável pela direção estratégica de TI nos departamentos em que a área da “Gestão de *Facilities*” presta serviços,
- ♦ **Superintendência Executiva** – responsável pela administração estratégica de TI nas suas áreas específicas nos departamentos em que a “Gestão de *Facilities*” presta serviços;

Nível Estratégico de *Facilities*

- ♦ **Diretoria Departamental de *Facilities* (DDF)** – responsável pela direção estratégica de *Facilities*;
- ♦ **Superintendência Executiva de *Facilities* (SEF)** – responsável pela administração estratégica de *Facilities* sobre as suas áreas específicas no departamento de Gestão de *Facilities*;
- ♦ **Gerência Executiva de *Facilities* (GEF)** – responsável pela gestão técnica e administrativa da área de *Facilities* de Missão Crítica para TI nos Departamentos de Informática, bem como, a interação junto ao nível estratégico de TI dos departamentos que suporta, ou seja, todos os segmentos de Tecnologia da Informação da Organização;

Nível Tático de *Facilities*

- ♦ **Gerência de Planejamento, Automação e Controles (GPAC)** – responsável pelo gerenciamento técnico de planejamento, automação e controles, incluindo-se o processo de “Inteligência do Negócio & Gestão do Conhecimento (BI&KM)”, da área de Gestão de *Facilities* de Missão Crítica para TI;
- ♦ **Gerência de Operação, Manutenção e Instalações (GOMI)** - responsável pelo gerenciamento técnico de operação, manutenção e instalações nos ambientes físicos sob a jurisdição da área Gestão de *Facilities* de Missão Crítica, bem como, a interação junto aos demais gestores da Organização em questões operacionais que possam envolver impactos negativos ao funcionamento ininterrupto dos equipamentos e funções estratégicas de TI;

Nível Operacional de *Facilities*

- ♦ **Coordenadoria de Apoio Administrativo** – responsável pela coordenação administrativa dos assuntos estratégicos em nível executivo da área Gestão de *Facilities* de Missão Crítica para TI;
- ♦ **Coordenadoria de Planejamento** - responsável pela coordenação em projetos de planejamento de sistemas ou soluções em *Facilities* de Missão Crítica para TI;
- ♦ **Coordenadoria de Automação** – responsável pela coordenação em projetos de automação das soluções em *Facilities* de Missão Crítica para TI;
- ♦ **Coordenadoria de Controles** - responsável pela coordenação em projetos de controles para as soluções em *Facilities* de Missão Crítica para TI, incluindo-se os controles de “*compliance*” (aderência às normas técnicas e legislações vigentes) e de “*performance*” (indicadores de desempenho);
- ♦ **Coordenadoria de “BI&KM” (Inteligência do Negócio & Gestão do Conhecimento)** - responsável pela coordenação em projetos de “BI&KM” para as soluções em *Facilities* de Missão Crítica para TI, incluindo-se os processos de disponibilização e acompanhamento de uso dos meios para facilitar a busca de inovações, produtos e serviços que possibilitem o constante trabalho de crescimento e desenvolvimento pleno do potencial da equipe de trabalho da área;
- ♦ **Coordenadoria CPD Site Principal** – responsável pela coordenação técnica operacional (O,M&I-Operação, Manutenção e Instalações) dos sistemas de *Facilities* de Missão Crítica nos espaços construídos ocupados pelos Departamentos de Informática alocados na sede Matriz da Organização;
- ♦ **Coordenadoria CPD Site de Contingência** - responsável pela coordenação técnica operacional (O,M&I) dos sistemas de *Facilities* de Missão Crítica nos espaços construídos ocupados pelos Departamentos de Informática, alocados na sede do “*site back-up*”;
- ♦ **Coordenadoria PSC (Pólos de Serviços Centralizados)** - responsável pela coordenação técnica operacional (O,M&I) dos sistemas de *Facilities* de Missão Crítica nos espaços construídos ocupados pelos Departamentos de Informática, alocados em sedes regionais de serviços centralizados (Nível Brasil);
- ♦ **Coordenadoria de PRA (Pólos Regionais de Atendimento)** - responsável pela coordenação técnica operacional (O,M&I) dos sistemas de *Facilities* de Missão

Crítica nos espaços construídos ocupados pelos ambientes de automação e informática, alocados em sedes regionais de atendimento (Nível Brasil);

Totalização dos Recursos Humanos Propostos

Assim considerado, o novo organograma do TI-Gestão de *Facilities*, ou simplesmente TI-GFAC, pode ser concebido para um quadro interno de funcionários contando-se um total mínimo de 32 (trinta e dois) postos de trabalho (pt), sendo, 01 pt de “Diretor Departamental de *Facilities*” (DDF), 01 pt de “Superintendente Executivo de *Facilities*” (SEF), 01 pt de “Gerente Executivo de *Facilities*” (GEF), 02 pt de “Gerente de *Facilities*” (GPAC e GOMI), 08 pt de “Coordenador de *Facilities*” (08 coordenadorias específicas descritas acima), 16 pt de “Analista de *Facilities*” (distribuídos em dupla para cada coordenadoria descrita acima), 01 pt de “Coordenador de Apoio Administrativo” (01 coordenadoria específica descrita acima) e 02 pt de “Assistente de Apoio Administrativo” (dupla que se reporta à coordenadoria de apoio administrativo). Neste modelo, todos os demais cargos e funções devem ser supridos via processos de terceirizações, mediante uma reestruturação específica deste, visando incluir um novo modo operacional através do modelo de gestão especializada de terceiros em substituição ao eventual modelo de autogestão vigente.

6.3.6 Conjunto de Premissas Básicas do TI-GFAC

- ♦ “As recomendações da **ABNT-Associação Brasileira de Normas Técnicas e Legislações Vigentes** são o padrão mínimo necessário ao adequado desempenho das funções de **Gestão de *Facilities*** de Missão Crítica para TI”;

- ♦ “A **Engenharia em *Facilities*** de Missão Crítica para TI se faz acima do padrão mínimo estabelecido pelas exigências requeridas por normas técnicas da ABNT e Legislações Vigentes”;
- ♦ “A **Gestão de *Facilities*** de Missão Crítica para TI visa promover a **Interação PPP – Pessoas, Processos e Propriedades**”;
- ♦ “A propriedade é o **espaço construído** ou sistema predial e seus subsistemas, bem como, a **informação sobre os ativos físicos** dos complexos submetidos ao processo de **Gestão de *Facilities*** de Missão Crítica para TI”;
- ♦ “A **garantia de qualidade** no processo de provimento das soluções de *Facilities* de Missão Crítica para TI, envolve, no mínimo, cinco pontos básicos de avaliação de conformidade através de ensaios específicos, a saber - de tipo; de rotina; de comissionamento; de certificação; de manutenção – conforme estabelecido em um modelo processual definido para criar uma base de **Governança em *Facilities***”.

6.3.7 Essência da Governança em *Facilities*

O processo de provimento das soluções técnicas em *Facilities* de Missão Crítica (FMC) para Tecnologia da Informação (TI), visando garantir a máxima confiabilidade dos sistemas e/ou soluções técnicas (alta disponibilidade : de funcionamento dos ativos e de flexibilidade para mudanças), constitui-se de um conjunto de ações definidas com o objetivo de criar uma base de **Governança em *Facilities***, conforme etapas básicas descritas a seguir.

RFP/RFI : desenvolvimento e envio ao Departamento de Compras da RFP-*Request for Proposal* (definição de requisitos técnicos para a cotação do sistema e/ou solução técnica) e da RFI-*Request for Information* (definição do conjunto de informações comerciais, referenciais de mercado, de responsabilidade social e ambiental requeridas das empresas pretendentes à concorrência);

Projeto : desenvolvimento do conjunto de idéias e suas representações gráficas em desenhos, cortes, plantas, detalhes, dentre outros;

Protótipo : desenvolvimento de corpo físico preliminar conforme detalhado em projetos visando facilitar as análises e ensaios experimentais do sistema e/ou solução técnica proposta;

Ensaio de Tipo* : destina-se ao primeiro nível de verificações de conformidade com os requisitos colocados para um determinado tipo de sistema e/ou solução técnica, descritos na RFP de base para as cotações de preços;

Produtos em Série : desenvolvimento e disponibilização dos elementos em série, conforme detalhamentos em projetos e resultados obtidos com o protótipo, os quais visam possibilitar a fabricação da solução técnica e/ou sistema a ser fornecido ao cliente final;

Fabricação : produção em série dos sistemas e/ou soluções técnicas ofertados e negociados junto ao cliente final;

Ensaio de Rotina* : destina-se ao segundo nível de verificações de conformidade com os requisitos colocados para um determinado tipo de sistema e/ou solução técnica, descritos na RFP de base para as cotações de preços;

Transporte : procedimentos para a entrega dos sistemas e/ou soluções técnicas no destino final requerido pelo cliente que deve constar da RFP;

Instalação : procedimentos de montagens para instalação do sistema e/ou solução técnica fornecidos pelo fabricante;

Ensaio de Recebimento (Comissionamento)* : destina-se ao terceiro nível de verificações de conformidade com os requisitos colocados para um determinado tipo de sistema e/ou solução técnica, descritos na RFP de base para as cotações de preços;

Ativação : procedimentos para o *star-up* (ativação) do sistema e/ou solução técnica fornecidos pelo fabricante;

Projeto *As Built* : desenvolvimento de atualizações do conjunto de representações gráficas das idéias aplicadas no sistema e/ou solução técnica fornecidos pelo fabricante, mediante revisão dos desenhos, cortes, plantas, detalhes, dentre outros;

Inspeção Sistêmica : procedimentos para verificações do funcionamento do sistema e/ou solução técnica em conjunto aos demais sistemas interdependentes ou pertencentes à sua envoltória, avaliando-se os resultados e os impactos;

Ensaio de Certificação/Etiquetagem* : destina-se ao quarto nível de verificações de conformidade com os requisitos colocados para um determinado tipo de sistema e/ou solução técnica, descritos na RFP de base para as cotações de preços;

Início de Operação : colocação do sistema e/ou solução técnica fornecida em regime de produção, conforme capacidade especificada nos requisitos que constaram da RFP, projetos, ensaios e demais etapas anteriores deste processo de garantia da qualidade;

ULC-*Usefull Life Cycle* (Ciclo de Vida Útil) : período máximo especificado para utilização do sistema e/ou solução técnica, o qual compreende desde a fase de concepção, operação, manutenção e até a fase de disposição;

Ensaio Periódicos de Manutenção* : destina-se ao quinto nível de verificações de conformidade com os requisitos colocados para um determinado tipo de sistema e/ou solução técnica, descritos na RFP de base para as cotações de preços;

(*) Pontos Essenciais de Avaliação de Conformidade, prioritários ao acompanhamento pela Gestão de *Facilities* (representantes ou seus prepostos), visando a Garantia de Qualidade nas funções para as quais o sistema e/ou solução técnica foram projetados, sob pena de serem prejudicados os indicadores de desempenho e/ou a segurança operacional esperados, cujos efetivos controles (procedimentos e informações) constituem-se a base do processo de Governança em *Facilities*.

O modelo básico de Governança em *Facilities* ora proposto, destina-se a garantir a segurança operacional dos ativos físicos objeto da Gestão Completa de Infra-estrutura e Instalações, em níveis coerentes às mais elevadas expectativas definidas em projetos de sistemas e/ou soluções técnicas de FMC-*Facilities* de Missão Crítica

para TI, visando corresponder aos desafios impostos por exigências formuladas nas mais diversas fontes, tais como: agências reguladoras, associações, institutos, legislações específicas, acordos, tratados, normativas técnicas, padrões de qualidade, desempenho, confiabilidade, disponibilidade, flexibilidade, sustentabilidade, dentre outros.

Cabe ressaltar ainda, o contexto atual das organizações onde a necessidade de imprimir e demonstrar os controles dos seus pilares essenciais – Pessoas, Processos e Propriedades - fez nascer o conceito de **Governança Corporativa**, o qual encontrou elevada dependência de Tecnologia da Informação, portanto, desencadeou o surgimento do processo complementar de **Governança em TI**, da mesma forma, a Tecnologia da Informação encontra a sua base de sustentação nos ativos físicos de infra-estrutura e instalações, cujo funcionamento adequado, ininterrupto e com alternativas flexíveis para manutenções sem implicar em interrupções para a carga crítica (TI), constitui-se o grande desafio do processo definido como **Governança em Facilities**, ou seja, o maior objetivo da **Gestão de Facilities** de Missão Crítica para TI.

6.3.8 Plano de Cargos e Funções

O conjunto de cargos e funções, incluindo-se o descritivo de perfil e experiência dos profissionais para a formulação de uma matriz de postos de trabalho e suas respectivas modulações em graus de hierarquia, isso tudo, constituindo-se um “Plano de Cargos e Funções” que permita, posteriormente, definir um “Plano de Carreira, Salários e Treinamento” para a equipe técnica e administrativa do **TI-Gestão de Facilities** ou simplesmente **TI-GFAC**, ora se faz expresso nas formulações a seguir.

❖ GERENTE EXECUTIVO DE *FACILITIES*

- **Trainee** – engenheiro inscrito no CREA (qualquer habilitação) ou técnico inscrito no CREA (qualquer habilitação) com nível superior em áreas multidisciplinares de interesse da Organização (administração, direito, economia, TI, arquitetura e outras) e pós-graduação em *Facilities* (ex: MBA/USP-Gerenciamento de Facilidades); inglês básico; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** - engenheiro inscrito no CREA (qualquer habilitação) com pós-graduação em *Facilities*; inglês intermediário; experiência profissional de 3 anos nesta área;
- **Senior** – perfil descrito para o nível “Pleno”; inglês avançado; experiência profissional de 5 anos na função;

Função : gerenciamento técnico e administrativo da área de Gestão de *Facilities* de Missão Crítica para TI em Instituição Financeira de Classe Mundial, facilitando as tratativas dos assuntos técnicos de *Facilities* com as funções estratégicas de Tecnologia da Informação.

❖ GERENTE DE *FACILITIES*

- **Trainee** – engenheiro inscrito no CREA (qualquer habilitação) ou técnico de nível médio inscrito no CREA (qualquer habilitação); inglês básico; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** – engenheiro inscrito no CREA (qualquer habilitação) ou técnico de nível médio inscrito no CREA (qualquer habilitação) e nível superior em áreas de interesse do Banco (administração, direito, economia, TI,

arquitetura e outras); inglês intermediário; experiência profissional de 3 anos na função;

- **Senior** – perfil descrito para o nível “Pleno” com pós graduação em *Facilities* (ex: MBA-USP/Gerenciamento de Facilidades); inglês avançado; experiência profissional de 5 anos na função;

Função : gerenciamento técnico em divisão operacional ou de planejamento da área de Gestão de *Facilities* de Missão Crítica para TI.

❖ COORDENADOR DE *FACILITIES*

- **Trainee** – engenheiro/arquiteto inscrito no CREA (qualquer habilitação) ou técnico de nível médio inscrito no CREA (qualquer habilitação); inglês básico; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** – engenheiro/arquiteto inscrito no CREA (qualquer habilitação) ou técnico de nível médio inscrito no CREA (qualquer habilitação) e nível superior em áreas de interesse do Banco (administração, direito, economia, TI, arquitetura e outras); inglês intermediário; experiência profissional de 3 anos na função;
- **Senior** – perfil descrito para o nível “Pleno” com experiência profissional de 5 anos na função ou pós-graduado em *Facilities* (ex: MBA-USP/Gerenciamento de Facilidades) com experiência profissional de 3 anos na função; inglês avançado em ambos os casos;

Função : coordenação técnica dos projetos de sistemas e/ou soluções técnicas em *Facilities* de Missão Crítica para TI.

❖ ANALISTA DE *FACILITIES*

- **Trainee** – tecnólogo ou técnico de nível médio inscrito no CREA (qualquer habilitação); noções de inglês; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** – tecnólogo ou técnico de nível médio inscrito no CREA (qualquer habilitação) e nível superior em áreas de interesse do Banco (administração, direito, economia, TI, arquitetura e outras); inglês básico; experiência profissional de 3 anos na função;
- **Senior** – perfil descrito para o nível “Pleno” com experiência profissional de 5 anos na função ou pós-graduado em *Facilities* (ex: MBA-USP/Gerenciamento de Facilidades) com experiência profissional de 3 anos na função; inglês intermediário em ambos os casos;

Função : análise, suporte técnico e acompanhamento dos projetos de sistemas e/ou soluções técnicas em *Facilities* de Missão Crítica para TI.

❖ COORDENADOR ADMINISTRATIVO EM *FACILITIES*

- **Trainee** – graduação de nível médio ou superior em áreas multidisciplinares de interesse do Banco; noções de inglês; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** – graduação de nível superior em áreas multidisciplinares de interesse do Banco; inglês básico; experiência profissional de 3 anos na função;
- **Senior** – perfil descrito para o nível “Pleno” com experiência profissional de 5 anos na função ou pós-graduado em áreas multidisciplinares de interesse do Banco com experiência profissional de 3 anos na função; inglês básico em ambos os casos;

Função : coordenação administrativa dos assuntos estratégicos da área de Gestão de *Facilities* de Missão Crítica para TI.

❖ ASSISTENTE ADMINISTRATIVO EM *FACILITIES*

- **Trainee** – graduação de nível médio em áreas multidisciplinares de interesse do Banco; noções de inglês; experiência profissional de 2 anos nesta área;
- **Junior** – perfil descrito para o nível “Trainee”; experiência profissional de 2 anos na função;
- **Pleno** – perfil descrito para o nível “Trainee”; experiência profissional de 3 anos na função;
- **Senior** – perfil descrito para o nível “Trainee” com experiência profissional de 5 anos na função ou graduação de nível superior em áreas multidisciplinares de interesse do Banco; com experiência profissional de 3 anos na função; inglês básico em ambos os casos;

Função : assistência administrativa e acompanhamento dos assuntos estratégicos da área de Gestão de *Facilities* de Missão Crítica para TI.

6.3.9 Consolidação

O presente Plano de Reestruturação da Infra-estrutura existente não tem a pretensão de esgotar as possibilidades de apresentação de idéias para a reestruturação da Área de Infra-estrutura e Instalações para TI, que, conforme proposto e desde logo, foi tratado com a nova denominação de **TI-Gestão de *Facilities*** ou simplesmente **TI-GFAC**, portanto, uma vez admitida a hipótese de serem aceitas as sugestões ora formuladas, tão logo quanto possível aos profissionais destacados para ocuparem os cargos propostos, deve ser elaborado um Planejamento Estratégico desta nova área, considerando todo o exposto ora apresentado.

O conceito de “**Gestão de *Facilities***” demonstra-se muito simples em sua forma quando entendido como um conjunto de recursos que, uma vez disponibilizados, permitem garantir a segurança operacional e máxima condição de ininterruptibilidade das funções de TI para o suporte e alavancagem de negócios da Organização.

Afinal, longe de ter um fim, esse é um processo perene e que vai obrigar a equipe de *Facilities* de Missão Crítica (FMC) para TI, a se superar e melhorar sempre, o que se acredita ser possível com a significativa contribuição que poderá ser evidenciada a partir da implementação do conceito de “**Governança em *Facilities***”, objeto de abordagem preliminar neste documento.

Assim, a partir deste trabalho, fica submetido o plano básico para reestruturação da Área de Infra-estrutura e Instalações, desde logo tratada com a nova denominação de **TI-Gestão de *Facilities*** ou simplesmente **TI-GFAC**, uma vez consideradas válidas as idéias e os argumentos apresentados, além de, cumpridos todos os trâmites necessários que possibilitem levar a termo a autorização pretendida.

Um conjunto de documentos anexos ao presente Plano de Reestruturação da Infra-estrutura existente pode oferecer maiores subsídios quanto ao assunto “**Gestão de *Facilities***”, mediante a disponibilização de matérias com o enfoque da mídia especializada neste seguimento (ex: citar publicações com destaque para os “*Facility Managers*” ou “Gerentes de *Facilities*”), além de, salientar eventuais publicações acadêmicas (ex: acervo da Escola Politécnica de Engenharia da Universidade de São Paulo) contendo uma série de conceitos sobre o **Gerenciamento de *Facilities*** para aplicação em edificações produtivas.

CONCLUSÃO

Este estudo procurou abordar de maneira estruturada e analítica as diversas legislações específicas de impacto no setor bancário, sob uma abordagem aos conceitos necessários para o suporte e planejamento dos sistemas de Gerenciamento de Facilidades de Missão Crítica em edificações de alto desempenho e de elevada criticidade, além de oferecer um panorama de TI e o contexto para o desenvolvimento de uma proposta de Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras.

A modalidade gerencial dos ativos físicos de infraestrutura e instalações no setor bancário foi estruturada, sendo propostas as bases de um programa visando utilizar o Gerenciamento de Facilidades como alavanca de negócios das Organizações, o que incluiu os elementos que possibilitam este entendimento e os meios necessários para atingir os objetivos propostos, visando garantir as certificações de que as efetivas melhorias de controle dos riscos de segurança da informação encontram-se adequadamente implementadas inclusive para os ativos físicos da Organização, cujo complexo de recursos também podem ser reforçados para se enfrentar os novos desafios impostos às Instituições Financeiras de Classe Mundial.

O primeiro capítulo abordou uma descrição preliminar de como os ativos físicos, tais como propriedades, edifícios, equipamentos, materiais e móveis representam significativos montantes dos custos anuais de manutenção e relevante percentual de participação nos ativos totais das organizações, principalmente no Gerenciamento de Facilidades Prediais de Missão Crítica nos ambientes de TI de Instituições Financeiras. Adicionalmente, uma abordagem ao contexto legislativo do setor bancário procurou oferecer uma visão das mais novas e complexas exigências para as Instituições Financeiras que atuam no mercado globalizado, passando pelas mais variadas normas e regulamentos exigidos por auditorias internas e externas que visam evidenciar os procedimentos adotados pela organização para oferecer

desempenho e aderência aos diversos dispositivos regulatórios deste mercado, onde tais necessidades fundamentam as bases da Governança Corporativa e da Governança em TI, as quais ora precisam contar com os mais efetivos controles dos ativos físicos da empresa e, assim, torna o momento oportuno para se desenvolver os conceitos e uma proposta de Modelo de Governança em *Facilities*.

No segundo capítulo, foram vistos os componentes principais do panorama atual de Tecnologia da Informação, incluindo análises sobre a gestão de segurança da informação e conceitos de Facilidades Prediais de Missão Crítica que descreveram o novo paradigma estabelecido pela Governança em TI de Instituições Financeiras, onde questões fundamentais, como a natureza intangível de muitos dos resultados esperados, precisam ser endereçadas com a aplicação de novas técnicas de gestão, o que não poder ser diferente na Gestão de *Facilities* em ambientes de Missão Crítica. A “Pirâmide de Tecnologia da Informação” demonstrou o elevado nível de dependência de TI evidenciado no setor bancário, bem como, o elevado nível de dependência de *Facilities* no segmento de TI em Instituições Financeiras. As análises sobre a gestão de segurança da informação demonstraram os diversos fatores de riscos e ameaças que podem ser identificadas nos ambientes físicos de CPD, as quais requerem as mais diversas ações da Gestão de *Facilities* para garantir a segurança operacional dos ambientes de Missão Crítica, os quais também foram alvo das considerações sobre as frentes de trabalho neste mercado que visam estabelecer de forma definida e balanceada os parâmetros para a classificação do desempenho físico em ambientes de CPD.

No terceiro capítulo, foram apresentados os conceitos de Planejamento Estratégico aplicados no Gerenciamento de Facilidades de Missão Crítica para TI, com a visão de um diagnóstico geral alinhado às necessidades de todas as áreas de Tecnologia da Informação da organização, objetivando imprimir excelência na prestação dos serviços de TI aos seus clientes internos e externos. Foram abordados os principais pontos do planejamento de *Facilities*, tais como os Gerenciamentos de Valores, de Qualidade, de Riscos, de Mudanças e o Ambiental, resultando numa ampla gama de análises situacionais, de metodologias e de resultados esperados.

No quarto capítulo, foram abordadas as questões de especificações de padrões prediais nos ambientes de Missão Crítica para TI onde foi possível verificar que a flexibilidade constitui-se qualidade fundamental de projeto que facilitam as mudanças em Centros de Tecnologia da Informação, além de, terem sido abordados todos os aspectos ideais aos sistemas prediais de um CPD, desde as diretrizes construtivas, o fornecimento e distribuição de energia com os seus diagramas e detalhamentos especiais, os sistemas de climatização/ventilação/resfriamento considerando as questões para qualidade do ar e as necessidades específicas dos ativos de TI&Telecom, os diversos conceitos e dispositivos para a segurança física, o cabeamento lógico do CPD com ênfase nos cabos de cobre UTP e os sistemas de monitoração e inteligência predial.

No quinto capítulo, foram identificadas as informações necessárias aos Contratos no Gerenciamento de Facilidades com enfoque principal nos requisitos técnicos de qualificação dos fornecedores e dos aspectos específicos da prestação de serviços de projetos e gerenciamento de ambientes de Missão Crítica para TI, em abordagem aos diversos conjuntos de condições e estabelecimento de características referentes às obrigações das partes envolvidas, por meio de documentos denominados de RFP-*Request for Proposal* (Solicitação de Propostas) e RFI-*Request for Information* (Pedido de Informações dos Fornecedores).

No sexto capítulo, foram desenvolvidas as bases fundamentais de uma proposta de Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras, como sendo um terceiro elemento que também se faz necessário para contribuir na plena Governança das Organizações, alinhando-se aos conceitos de Governança Corporativa e de Governança em TI na qualidade de base fundamental para o desenvolvimento destas. Por ocasião do desenvolvimento de conceitos do Modelo de Governança em *Facilities* também foram analisadas as ferramentas de apoio automatizado (CAFG/CAFM) e foi apresentado um Plano de Reestruturação da Infra-estrutura Organizacional visando servir de referencial básico e avaliação dos recursos mínimos para se efetivar a implementação da Governança em *Facilities*.

Desta maneira, a chegada da nova economia preconizada por diversos autores que estabelece a informação como o único recurso realmente significativo, principalmente num cenário de elevada competitividade, mudanças de valores e paradigmas, impõe-se na globalização das economias, os conceitos de Governança Corporativa e Governança em TI, os quais também são dependentes de uma Governança em *Facilities*, como foi apresentado no presente trabalho sobretudo por ocasião da proposta de um Modelo de Governança em Facilidades Prediais para Centros de Tecnologia da Informação de Instituições Financeiras.

O objetivo deste estudo foi tratar os conceitos fundamentais do Gerenciamento de Facilidades aplicados em ambientes de Missão Crítica para TI, como resposta aos mais recentes desafios lançados ao setor bancário em âmbitos nacional e internacional, onde a necessidade de um efetivo controle das informações dos ativos físicos das organizações constitui-se fator crítico de sucesso com o propósito de atender uma ampla gama de exigências formuladas pelas mais diversas agências reguladoras, neste sentido, a proposta de um Modelo de Governança em Facilidades Prediais para os Centros de Tecnologia da Informação procurou descrever a visão da necessidade de uma estrutura organizacional autônoma e automatizada, com o reforço dos recursos que possibilitem manter a organização nas primeiras posições classificatórias do mercado, por meio de uma “Gestão Completa de Infra-estrutura e Instalações” em Instituições Financeiras de Classe Mundial.

“Não há nada mais poderoso do que uma idéia que chegou no tempo certo”

Victor Hugo

ANEXO A

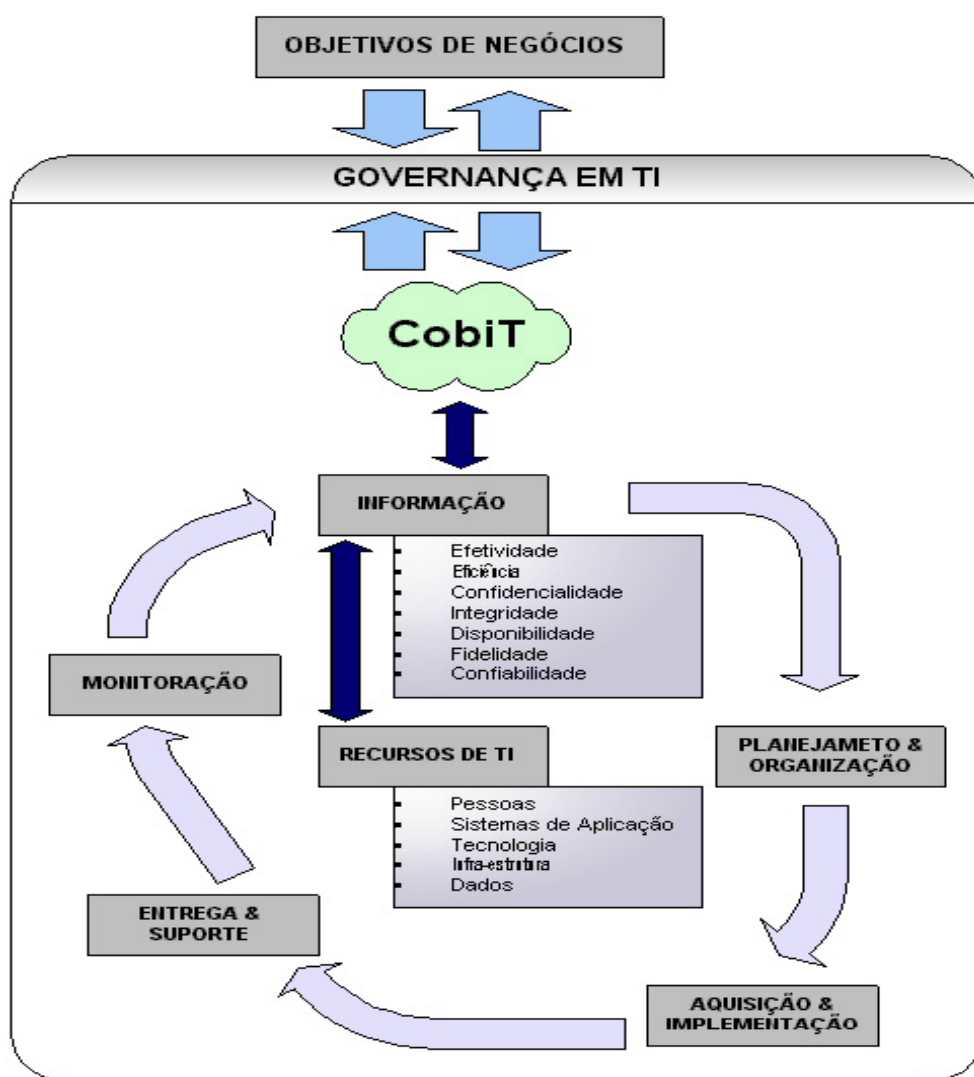
Caracterização do Sistema Predial Centro de Tecnologia da Informação

Fonte : ELLERBE BECKET



ANEXO B

Diagrama da Visão para Governança em TI

Fonte : COBIT

ANEXO C

Características Funcionais dos Sistemas Prediais

Fonte : GONÇALVES (1999)

Sistemas Prediais	Flexibilidade	Confiabilidade	Gerenciamento
Sistemas de Suprimento de Energia	Shafts, dutos Modularidade Cablagem Dutagem	Alimentação Alternativa Geradores No-breaks Baterias <i>stand-by</i>	Administrativo Conservação de Energia Fontes Alternativas Operação/Manutenção
Sistemas de Suprimento e Disposição de Águas	Espaços Modularidade Dutagem	Alimentação Alternativa Equipamentos <i>stand-by</i>	Administrativo Uso Racional da Água Operação Manutenção
Sistemas de Segurança	Modularidade Acessibilidade Cablagem Dutagem	Fontes Ininterruptas Cruzamento de Informações Rotina de Testes	Administrativo Técnico Operação Manutenção
Sistemas de Conforto Ambiental	Modularidade Pré-cablagem Dutagem Espaços	Equipamentos stand-by Alimentação Alternativa Setorização	Administrativo Energético Operação Manutenção
Sistemas de Transporte	Espaços Equipamentos Cablagem	Alimentação Alternativa Setorização	Fluxo Administrativo Operação Manutenção
Sistemas de Comunicação	Espaço Modularidade Cablagem	Equipamentos stand-by Alimentação Alternativa Protocolos	Administrativo Interface Operação Manutenção
Sistemas de Automação	Espaços Modularidade Cablagem Dutagem Remotos	Alimentação Alternativa Protocolos Setorização	Auto-gerenciamento

ANEXO D

Gerenciamento de Facilidades – Funções e Responsabilidades

Fonte : IFMA (2004)

Operações de Manutenção ◆ Manutenção de mobiliário ◆ Manutenção de revestimentos ◆ Manutenção preventiva ◆ Manutenção corretiva ◆ Manutenção de fachadas ◆ Zeladoria e limpeza ◆ Manutenção de jardins	Serviços Administrativos ◆ Material fotográfico corporativo ◆ Serviços de mensagens ◆ Envio/Recebimento ◆ Conservação de arquivos ◆ Segurança ◆ Telecomunicações ◆ Cópias Reprográficas
Gerenciamento de Espaço ◆ Inventário de Espaço ◆ Políticas para Espaços ◆ Alocação de Espaços ◆ Controle de Mobiliário ◆ Reformas (retrofits) ◆ Resíduos e lixo sólido ◆ Materiais Perigosos	Imóveis ◆ Aluguel de Edifícios ◆ Seleção de Locais ◆ Aquisição ◆ Demolição ◆ Avaliação de Propriedades ◆ Sub-locações
Saúde e Segurança ◆ Ergonomia ◆ Qualidade do Ar Interno ◆ Reciclagem de Resíduos ◆ Emissões de Poluentes	Arquitetura e Engenharia ◆ Conformidade às Normas ◆ Projetos ◆ Construções ◆ Sistemas Prediais
Planejamento Operacional ◆ Operação de Sistemas ◆ Plano de Emergências ◆ Plano Estratégico ◆ Plano Energético	Planejamento Financeiro ◆ Previsão Orçamentária ◆ Programa de Capital ◆ Financiamentos

REFERÊNCIAS BIBLIOGRÁFICAS

1. ACKOFF, RUSSEL L. **Re-creating Corporation – A design of organizations for 21st Century**. Oxford University Press, Oxford, 1999.
2. GRAÇA, MOACYR EDUARDO ALVES DA. **Formulação de modelo para avaliação das condições determinantes de necessidade de ventilação secundária em sistemas prediais de coleta de esgotos sanitários**. São Paulo, 1985, Tese (Doutorado) – Escola Politécnica da Universidade de São Paulo.
3. ANTONIOLI, PAULO EDUARDO. **Estudo crítico sobre subsídios conceituais para suporte do planejamento de sistemas de gerenciamento de facilidades em edificações produtivas**. São Paulo, 2003, Tese (Mestrado) – Escola Politécnica da Universidade de São Paulo.
4. INTERNATIONAL FACILITIES MANAGEMENT ASSOCIATION-EUA. **Associação Internacional de Gerenciamento de Facilidades**, disponível em <http://www.ifma.com>, acessado em 18 de fevereiro de 2005.
5. TEICHOLZ, ERIC. **Facility Design and Management Handbook**. McGraw-Hill, New York, 2001.
6. REVISTA EXECUTIVOS FINANCEIROS. **Publicação do Setor Bancário**, disponível em <http://www.executivosfinanceiros.com.br>, acessado em 18 de fevereiro de 2005.
7. REVISTA BANCO HOJE. **Publicação do Setor Bancário**, disponível em <http://www.bancohoje.com.br>, acessado em 18 de fevereiro de 2005.
8. COMUNIDADE DA LISTA DE RISCOS. **Entidade que trata questões de Gestão de Risco**, disponível em <http://www.listaderiscos.com.br>, acessado em 18 de fevereiro de 2005.

9. LEX EDITORA. **Entidade nacional que efetua publicações no ramo do Direito**, disponível em <http://www.lex.com.br>, acessado em 20 de março de 2005.
10. COSO-COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. **Entidade que trata questões de Governança Corporativa**, disponível em <http://www.coso.org> acessado em 20 de março de 2005.
11. REVISTA TI. **Publicação de Tecnologia da Informação**, disponível em <http://www.timaster.com.br>, acessado em 20 de março de 2005.
12. EQUATOR PRINCIPLES. **Princípios do Equador, Conjunto de Princípios de Sustentabilidade para Instituições Financeiras**, disponível em <http://www.equator-principles.com>, acessado em 24 de abril de 2005.
13. IT GOVERNANCE INSTITUTE. **Instituto de Governança em TI**, disponível em <http://www.itgi.org>, acessado em 24 de abril de 2005.
14. PRITCHARD CARL L. **Risk Management Concepts and Guidance**. Editora ESI International, 1997.
15. BERTALANFFY, LUDIWIG VON. **Teoria Geral dos Sistemas**. Editora Vozes Ltda, Petrópolis, 1977.
16. ABCR-ASSOCIAÇÃO BRASILEIRA DE CAPITAL DE RISCO. **Associação nacional que trata de Gestão de Riscos**, disponível em <http://www.abcr-venture.com.br>, acessado em 24 de abril de 2005.
17. GESTÃO DE CRISES. **Universidade McMaster – Grupo do Gerenciamento de Crises**, disponível em <http://www.mcmaster.ca/newsevents/crisismanagement>, acessado em 18 de fevereiro de 2005.
18. GUSTIN, J. **Disater & Recovery Planning : a guide for facilities managers**. Farrmont Press, 2ed, 2002.
19. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799. **Tecnologia da Informação – Código de prática para a gestão de segurança da informação**. Rio de Janeiro, 2005.

20. LEVIT, ALAN M. **Disaster Planning and Recovery, A Guide for Facility Professionals**. John Wiley & Sons, 1997.
21. ACECOTI. **Empresa Especializada em Produtos e Serviços de Facilidades de Missão Crítica**, disponível em <http://www.acecoti.com.br>, acessado em 29 de maio de 2005.
22. HESKET, JAMES L. SASSER JR. W, EARL. HART, CHRISTOPHER W.L. **Serviços Revolucionários: mudando as regras do jogo**. São Paulo, Pioneira, 1994.
23. ZUFFO, JOÃO ANTONIO. **A Infoera – O imenso desafio do futuro**. Editora Saber Ltda., São Paulo, 1997.
24. MUSEU DO COMPUTADOR. **Associação Cultural de Registro da História da Informática**, disponível em <http://www.museudocomputador.com.br>, acessado em 24 de maio de 2005.
25. ELLERBE BECKET INC EUA. **Empresa Especializada em Projetos de Facilidades de Missão Crítica**, disponível em <http://www.ellerbebecket.com>, acessado em 18 de fevereiro de 2005.
26. UPTIME INSTITUTE EUA. **Grupo de Profissionais em Facilidades de Missão Crítica**, disponível em <http://www.uptimeinstitute.com>, acessado em 18 de fevereiro de 2005.
27. IEEE STD 493-1990, GOLD BOOK. **Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems**. Publicação do IEEE-Institute of Electrical and Eletronic Engineers Inc, EUA, 1990.
28. KAPLAN, ROBERT S. NORTON, DAVID P. **A Estratégia em Ação**. Rio de Janeiro : Campus, 1997.
29. INDG-INSTITUTO DE DESENVOLVIMENTO GERENCIAL. **Organização de Consultoria em Gestão Empresarial**, disponível em <http://www.indg.com.br>, acessado em 26 de junho de 2005.
30. PMBOK 2004. **A Guide to the Project Management Body of Knowledge – NBR ISO 10006**. Publicação do PMI-Project Management Institute, 2004.

31. TEICHOLZ, ERIC – FM TECHNOLOGY : GENERATION NEXT. **Facilities Design & Management**, disponível em <http://www.fmlink.com>, acessado em 26 de junho de 2005.
32. DCUG-DATA CENTER USER'S GROUP EUA. **Grupo de Profissionais Usuários de Data Center**, disponível em <http://www.datacenterug.org>, acessado em 27 de novembro de 2005.
33. CATERPILLAR, INC EUA. **Empresa Especializa em Soluções de Energia, Geradores e outros produtos em Facilidades de Missão Crítica**, disponível em <http://www.cat.com> e <http://brasil.cat.com> , acessados em 26 de junho de 2005.
34. LIEBERT CORPORATION/EMERSON NETWORK POWER-EUA. **Grupo de Empresas Especializadas em soluções de energia, no-break, climatização e outros produtos em Facilidades de Missão Crítica**, disponível em <http://www.liebert.com> e <http://www.liebert.com.br> , acessados em 18 de fevereiro de 2005.
35. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR 5674. **Manutenção de Edificações – Procedimento**. Rio de Janeiro, 1999.
36. IEEE STD 1100-1992, EMERALD BOOK. **Recommended Practice for Powering and Grounding Sensitive Electronic Equipment**. Publicação do IEEE-Institute of Electrical and Electronic Engineers Inc, EUA, 1992.
37. WHOLE BUILDING DESIGN GUIDE. **Organização que promove conceitos de projeto e construção de edifícios**, disponível em <http://www.wbdg.org>, acessado em 24 de julho de 2005.
38. EYP MISSION CRITICAL FACILITIES INC, EUA. **Empresa Especializada em Projetos de Facilidades de Missão Crítica**, disponível em <http://www.eypmcf.com> , acessado em 18 de fevereiro de 2005.
39. ANVISA-AGÊNCIA NACIONAL DE VIGILÂNCIA SANITÁRIA. **Entidade governamental que regula as questões de saúde pública**, disponível em <http://www.anvisa.gov.br>, acessado em 27 de fevereiro de 2005.

40. HOLDER CONSTRUCTION COMPANY, EUA. **Empresa Especializada em Gerenciamento e Construções de Data Centers**, disponível em <http://www.holder.com> acessado em 27 de fevereiro de 2005.
41. BEARG, DAVID W. **Indoor Air Quality and HVAC Systems**. Lewis Publishers, Boca Raton, 1993.
42. TORRES, GABRIEL. **Redes de Computadores Curso Completo**. Editora Axcel Books, 2001.
43. PIPER, JAMES. **Understanding open protocols. Building Operating Management**, disponível em <http://www.facilitiesnet.com>, acessado em 21 de agosto de 2005.
44. LEIRIA, JERÔNIMO SOUTO. **Gerenciamento de Contratos : como contratar e gerenciar bens e serviços**. Editora Cultural Ltda, 2ª edição, 1993.
45. JUNGMAN, MILTON. **A influência da estrutura e da organização na qualidade do atendimento: um estudo de caso de serviços**. São Paulo, 2000, Dissertação (Mestrado) – Escola Politécnica da Universidade de São Paulo.
46. FRIDAY, STORMY – COTTS, DAVID. **Quality Facility Management – A Marketing and Customer Service Approach**. John Wiley & Sons Inc, New York, 1995.
47. SMITH, PAUL R. **Facilities Engineering and Management Handbook**. MacGraw-Hill, New York, 2000.
48. TECHOLZ, ERIC. **Facility Design and Management Handbook**. MacGraw-Hill, New York, 2001.
49. TUV RHEINLAND BRASIL. **Organismo para Certificação e Qualificação de Produtos e Serviços**, disponível em <http://www.tuvbrasil.com.br> , acessado em 04 de setembro de 2005.
50. WIREMAN, TERRY. **Developing Performance Indicators for Managing Maintenance**. Industrial Press Inc., New York, 1998.
51. BUILDING DESIGN & CONSTRUCTION MAGAZINE. **Publicação sobre projeto e construções de edifícios**, disponível em <http://www.bdcmag.com> , acessado em 04 de setembro de 2005.

52. U.S. GREEN BUILDING COUNCIL, EUA. **Conselho Americano do Edifício “Verde”**, disponível em <http://www.usgbc.com> acessado em 25 de setembro de 2005.
53. BREEAM-BUILDING RESEARCH ENVIROMENT ASSEMENT METHOD. **Organização que desenvolve Método de Pesquisa Ambiental para Edifícios**, disponível em <http://www.bream.org> acessado em 25 de setembro de 2005.
54. SISTENGE ENGENHARIA. **Empresa Especializada em Gerenciamento, Operação e Construção de CPD’s**, disponível em <http://www.sistenge.com>, acessado em 25 de setembro de 2005.
55. ARCHIBUS INC. **Empresa Especializada em Soluções de Software para Gerenciamento de Facilidades**, disponível em <http://www.archibus.com> e <http://www.grapho.com.br/archibus> , acessados em 18 de fevereiro de 2005.
56. APERTURE TECHNOLOGIES, INC. **Empresa Especializada em Soluções de Software para Gerenciamento de Infra-estrutura em Data Center**, disponível em <http://www.aperture.com> e <http://www.sparkel.com.br> , acessados em 25 de setembro de 2005.