SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GTL 15
14 a 17 Outubro de 2007
Rio de Janeiro - RJ

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

GESTÃO DA SEGURANÇA DA INFORMAÇÃO EM REDES CONVERGENTES OPERACIONAIS E CORPORATIVAS NO AMBIENTE CHESF

Rodrigo Leal de Siqueira (*) **Alexandre Wagner Dantas de Lira**

COMPANHIA HIDRO-ELÉTRICA DO SÃO FRANCISCO
CHESF

RESUMO

Em decorrência da convergência multifuncional e multiserviço das redes de telecomunicações, informática e automação da CHESF, e dos avanços tecnológicos permitindo que a informação esteja acessível dos pontos mais distantes pela rede *Internet*, *Intranet*, *Extranet*, acessos remotos, culminando com a tecnologia *Wireless,* observou-se a necessidade do estabelecimento de um Modelo de Referência para Gestão da Segurança da Informação no ambiente da CHESF.

Neste Informe Técnico (IT) é apresentado este modelo de referência, envolvendo os aspectos tecnológicos, físicos e humanos, com ênfase na rede operativa, e informando as medidas de segurança da informação planejadas pela Superintendência de Telecomunicações e Controle.

PALAVRAS-CHAVE

Segurança da Informação, Telecomunicações, Governança Corporativa, Informática, Convergência

1.0 - INTRODUÇÃO

No desenvolvimento de suas atividades de gestão empresarial, a CHESF necessita de um sistema de comunicações que atenda todas as suas necessidades corporativas e operacionais para tráfegos de informações, necessárias ao planejamento, projeto, construção, operação e manutenção do Sistema Eletro-Energético. Nos últimos 50 anos, foram implantados sistemas com domínios próprios, compostos por sistemas físicos, na maioria de sua propriedade, complementados por sistemas compartilhados com outras empresas ou alugados. Estes sistemas sempre que possível, acompanham o desenvolvimento tecnológico, sendo fundamental para obtenção dos níveis de serviço “contratado” (SLA, do inglês *service level agreement*) pelo sistema elétrico.

O sistema de telecomunicações da CHESF busca continuamente o desenvolvimento tecnológico e atualmente a convergência em soluções multiserviço, procurando a obtenção de níveis de desempenho, segurança e qualidade de serviço em atendimento aos seus requisitos. Tendo como premissa a evolução tecnológica e os aspectos de convergência, foi criado o Modelo de Referência para a Convergência de Informática, Telecomunicações e Automação na CHESF (MR-CITAC) para estabelecer os padrões que estão sendo perseguidos nesta fase. Neste modelo (1) é descrito a plataforma IP em operação e a projetada para a busca da convergência nas aplicações de sua tecnologia e processos. Neste IT será dada uma breve explanação sobre a composição do modelo para melhor entendimento dos conceitos apresentados posteriormente.

Em decorrência do avanço tecnológico e da “globalização” toda a informação está acessível dos pontos mais distantes pela rede *Internet*, *Intranet*, *Extranet*, acessos remotos, culminando com a tecnologia *Wireless*. A empresa virou uma grande teia de comunicação integrada, dependente do fluxo de informação que por ela é

(*) Rua Delmiro Gouveia, 333, Anexo 2, Bloco B, sala 334 – Recife – PE – Brasil
Tel.: (081) 3229.4165 Fax: (081) 3229.4216 E-mail: rodrigol@chesf.gov.br

distribuída e compartilhada, e essas informações agora sujeitas às vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e comportamentais. Considerando que as propriedades da informação (confidencialidade, integridade e disponibilidade) durante o seu ciclo de vida (manuseio, armazenamento, transporte e descarte) devem ser preservadas e protegidas das ameaças crescentes observou-se a necessidade de estabelecimento de um Modelo de Referência para Gestão da Segurança da Informação na CHESF (MR-GSIC) no ambiente administrativo e operacional.

Neste modelo é apresentada uma visão global da Gestão da Segurança da Informação no ambiente CHESF e as medidas de segurança planejadas, no âmbito da Superintendência de Telecomunicações e Controle (STC), para eliminar as vulnerabilidades e os furos de segurança, com a finalidade de obter os requisitos de segurança necessários para garantir a confiabilidade e disponibilidade indispensável ao Setor Eletro-Energético.

2.0 - COMPOSIÇÃO GERAL DO MODELO DE CONVERGÊNCIA

O estabelecimento do MR-CITAC considera como princípio absoluto a divisão do “Universo” em duas partes, sendo a primeira a “Something Else” formada por todas as outras coisas e a segunda, constituída pelo MR-CITAC. A “Something Else” na realidade forma o universo externo do MR-CITAC, tendo interfaces bem definidas com o mesmo, através das conexões existentes com a camada física, a camada de gestão e a camada de usuário. Este modelo é constituído por cinco camadas inter-relacionadas, como apresentado na Figura 1.

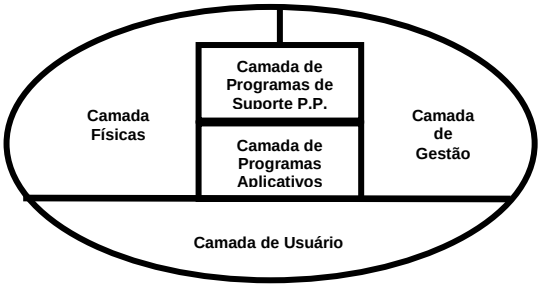

FIGURA 1: Composição do Modelo de Convergência

Este modelo foi comparado (1) com os Modelos de Referência OSI (*Open Systems Interconnection*) desenvolvido pela ISO (*International Standards Organization*) e com o Modelo de Referência TCP/IP. Neste modelo foi introduzidas duas novas camadas, ou seja, a camada de gestão e a camada de usuário.

2.1 Camada Física

A camada física tem como objetivo principal transmitir um fluxo bruto de bits de um processo de origem para um processo de destino, sendo composta pelo meio físico, sistema de transmissão, e infra-estrutura associada.

O meio físico é responsável pela prestação do serviço de fornecimento de um caminho entre o ponto transmissor e o ponto receptor. O modelo considerou as seguintes possibilidades de meio físico: espaço livre, linhas de transmissão, guias de onda, fios de cobre coaxias ou de pares trançados, e fibras ópticas.

Para a camada física, o sistema de transmissão é responsável pela transformação dos bits brutos recebidos de outras camadas do sistema de referência em sinais de informação compatíveis para transmissão no meio físico. A consideração da dimensão física nos leva a seguinte classificação para os sistemas de transmissão de acordo o meio físico utilizado: rotas de longa distância, enlaces de acesso e interligações de usuários.

O “hardware” da Infra-estrutura, dependendo do serviço que desenvolve em cada camada, pode assumir várias denominações e apresentar formas e características físicas as mais diversas, podendo se apresentar em duas formas operacionais: sem interface com o sistema elétrico (servidores, roteadores, etc.) ou com interface com o sistema elétrico (medidores, registradores etc.).

2.2 Camada de Programas de Suporte PP

A camada de programas de suporte PP consiste em “softwares” que permitem uma comunicação ponto a ponto eficiente e confiável, através da utilização da camada física. Esta camada realiza a detecção e correção de erros decorrentes de imperfeições no processo de transmissão pela camada física, regula o fluxo de dados, e é responsável pela função de comutação e roteamento, utilizando a comutação de pacotes “store-forward”.

2.3 Camada de Programas de Aplicativos

De natureza abstrata, a camada de programas aplicativos consiste em um conjunto de algoritmos traduzidos em “softwares” que permitem a transferência e processamento de dados confiável, econômico e eficiente entre a

máquina de origem e a máquina de destino. Esta camada é constituída basicamente por programas aplicativos da gestão empresarial, sob a responsabilidade da TI, programas aplicativos da gestão do sistema de telecomunicações e aplicativo de videoconferência sob a responsabilidade do Departamento de Telecomunicações e programas aplicativos operacionais sob a responsabilidade da Diretoria de Operação. Para melhor conhecimento dos programas de aplicativos utilizados na empresa podemos citar alguns exemplos, como: correio eletrônico (e-mail), WEB, PROD, áudio e vídeo digital compactado, VoIP, videoconferência sobre IP, SIGA, SAGE e SCADA.

2.4 Camada de Gestão

A camada de gestão é formada pelos programas aplicativos de uso exclusivo e o “Peapleware”, formado por profissionais voltados para os setores de Telecomunicações, Informática e Automação, sendo responsável pelas atividades de gerência, qualidade de serviço e segurança.

2.5 Camada de Usuário

A Camada de Usuário é composta de “User Peapleware”, ou seja, todos os gerentes e colaboradores pertencentes à CHESF, porém não pertencentes à camada de gestão, que usam serviços prestados por máquinas da Infra-estrutura da camada física e programas aplicativos da subcamada de aplicação.

3.0 - CONCEITOS DE SEGURANÇA DA INFORMAÇÃO

A Segurança da informação pode ser definida como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade, e de uma forma mais ampla, podemos considerá-la como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos de segurança:

a) Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo do seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas.
b) Integridade: Toda informação deve ser mantida ma mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-las contra alterações indevidas, intencionais ou acidentais.
c) Disponibilidade: Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários no momento em que os mesmos delas necessitem para qualquer finalidade.

Desta forma, estaríamos falando de definição de regras que incidiriam sobre todos os momentos do ciclo de vida da informação, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

3.1 Ativos

Os ativos são os elementos que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada.

Existem muitas formas de dividir e agrupar os ativos para facilitar seu tratamento: equipamentos, aplicações, usuários, ambientes, informações e processos. Desta forma, torna-se possível identificar melhor as fronteiras de cada grupo, tratando-as com especificidade e aumentando qualitativamente as atividades de segurança.

3.2 Aspectos da Segurança da Informação

Toda informação é influenciada por três propriedades principais, como mencionado, além dos aspectos autenticidade e legalidade que completam esta influência.

3.3 Ameaças

Agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração das vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade e, consequentemente, causando impactos aos negócios de uma organização, sendo classificadas quanto a sua intencionalidade nos seguintes grupos: naturais, involuntárias, e voluntárias.

3.4 Vulnerabilidades

Fragilidade presente ou associada à ativos que manipulam e/ou processam informações que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança. Como exemplos de vulnerabilidades, temos:

a) Físicas: Instalações fora do padrão, salas de CPD mal planejadas, falta de extintores, detectores de fumaça e de outros recursos para combate a incêndio em sala com armários e fichários estratégicos.

b) Naturais: Desastres naturais, falta de energia, acúmulo de poeira, aumento de umidade e de temperatura, etc.
c) Hardware: Falha nos recursos tecnológicos (desgaste, má utilização) ou erros durante a instalação.
d) Software: Erros podem gerar acessos indevidos, vazamento de informações, perda de dados, ou indisponibilidade dos recursos quando necessário.
e) Mídias: A radiação eletromagnética pode afetar diversos tipos de mídias comprometendo a informação.
f) Comunicação: Acessos não autorizados ou perda de comunicação.
g) Humanas: Falta de treinamento, compartilhamento de informações confidenciais, não execução de rotinas de segurança, erros ou omissões; ameaça de bomba, sabotagens, distúrbios civis, vandalismo, invasões, etc.

3.5 Medidas de Segurança

São as práticas, os procedimentos e os mecanismos usados para a proteção da informação e seus ativos, que podem impedir que ameaças explorem vulnerabilidades, a redução das vulnerabilidades, a limitação do impacto ou minimização do risco de qualquer outra forma, podendo ser classificadas em:

a) Preventivas: Políticas de segurança, procedimentos de trabalho, especificação de segurança, campanhas e palestras de conscientização de usuários; ferramentas de segurança (*firewalll*, antivírus, etc.)

b) Detectáveis: Análise de riscos, sistemas de detecção de intrusão, alertas de segurança, câmeras de vídeo.

c) Corretivas: Plano de Continuidade Operacional, Plano de Recuperação de Desastres.

3.6 Riscos

O risco é a probabilidade de que agentes, que são as ameaças, explorem vulnerabilidades, expondo os ativos a perdas de confidencialidade, integridade e disponibilidade, e causando impactos nos negócios. Estes impactos são limitados por medidas de segurança que protegem os ativos, impedindo que ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

$$\mathbf{R}_{\text{RISCO}} = \frac{\mathbf{V}_{\text{VULNERABILIDADE}} \times \mathbf{A}_{\text{AMEAÇA}} \times \mathbf{I}_{\text{IMPACTO}}}{\mathbf{M}_{\text{MEDIDA DE SEGURANÇA}}},$$

FIGURA 2: Diagrama da Equação de Risco de Segurança da Informação

3.7 Incidente

Fato (evento) decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda de princípios da segurança da informação: Confidencialidade, integridade e disponibilidade.

4.0 - GESTÃO CORPORATIVA DA SEGURANÇA DA INFORMAÇÃO

Há uma década a Chesf colocou em operação seu primeiro sistema transmissão digital, o qual contemplava inicialmente 29 pontos de presença de telecomunicações distribuídos na região nordeste, dando suporte às redes separadas de serviço de voz, dados e videoconferência. Em 2003 este sistema já atendia a 87,8% dos pontos de presença de telecomunicações, disponibilizando tributários de 2Mbits, utilizados pelos sistemas de telefonia com tecnologia TDM, canais dedicados de voz e dados utilizando tecnologia PCM, rede de longa distância utilizando tecnologia IP e rede de videoconferência utilizando canais dedicados. Neste mesmo período foram implantadas as primeiras LAN's na mesma seqüência em que os pontos de presença eram atendidos pelo sistema de transmissão digital, as quais apresentavam inicialmente redes de cabeamento estruturado categoria 5, fibras ópticas com terminações através de conversores de mídia e hubs. Durante o período de implantação das redes LAN's, em decorrência do avanço tecnológico, surgiu uma variada gama de novos equipamentos e soluções, os quais foram gradativamente adicionados às novas LAN's que iam sendo implantadas, tendo como resultado em 2006 uma plataforma de tecnologia IP heterogênea, sendo preparada para convergência multifuncional e multiserviço.

Atualmente o sistema de telecomunicações da CHESF atende a mais de 100 (cem) pontos de presença no Nordeste Brasileiro, incluindo subestações, usinas térmicas e hidroelétricas, repetidoras e escritórios administrativos, utilizando os recursos da camada física para prover comunicação corporativa e operacional necessárias ao desenvolvimento e sucesso do negócio. Em torno de 10% dos pontos de presença ainda são atendidos por canais alugados a prestadoras de serviço ou canais digitais do sistema OPLAT da CHESF.

Em decorrência do avanço tecnológico e da "globalização" toda a informação está acessível dos pontos mais distantes pela rede *Internet*, *Intranet*, *Extranet*, acessos remotos via VPN em dial-up ou em banda larga, culminando com a tecnologia *Wireless* fornecendo mobilidade. A empresa virou uma grande teia de comunicação integrada, dependente do fluxo de informação que por ela é distribuída e compartilhada, e essas informações agora sujeitas às vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e comportamentais. Diante do dinamismo dessas variáveis e considerando que as propriedades da informação durante o seu ciclo de vida devem ser preservadas e protegidas das ameaças

crescentes observou-se necessidade de estabelecimento de um Modelo de Referência para Gestão da Segurança da Informação na CHESF (MR-GSIC) no ambiente administrativo e operacional.

4.1 Modelo de Referência para Gestão da Segurança da Informação

Não basta criar um novo departamento ou unidade administrativa voltada à segurança da informação e chamá-lo de Comitê Corporativo de Segurança de Informação, é preciso ter uma visão clara de todas as etapas que compõem o desafio corporativo da segurança e formalizar os processos que darão vida e dinamismo a gestão.

A segurança deve ser mantida por um verdadeiro processo de gestão, sustentado por subprocessos retroalimentados, que interajam todo o tempo com as variáveis e estejam constantemente sendo ajustados às diretrizes estratégicas do negócio. Este modelo deve ser cíclico e encadeado, formado pelas etapas: Comitê de Segurança, Mapeamento da Segurança, Estratégia (Plano Diretor de Segurança), Planejamento (Política de Segurança da Informação), Implementação, Administração e Segurança na Cadeia Produtiva.

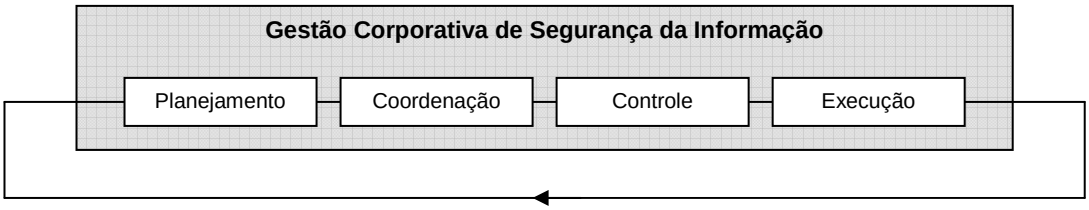

FIGURA 3: Processo de Gestão Cíclico Contínuo

Cada uma dessas etapas cumpre papel importante no ciclo e gera resultados finais que deverão estar devidamentes formatados para alimentar a etapa subseqüente. Desta forma será possível reagir com velocidade às mudanças que, inevitavelmente, ocorrerão na operação do negócio, fazendo o risco oscilar.

4.2 Composição do Modelo

O modelo é composto pela criação de uma estrutura corporativa adequadamente posicionada no organograma, chamada de Comitê Corporativo de Segurança da Informação, baseado em um modelo de gestão dinâmico, conforme apresentado na Figura 3, com autonomia e abrangência, coordenado por um executivo em ação focada, intitulado de Security Officer.

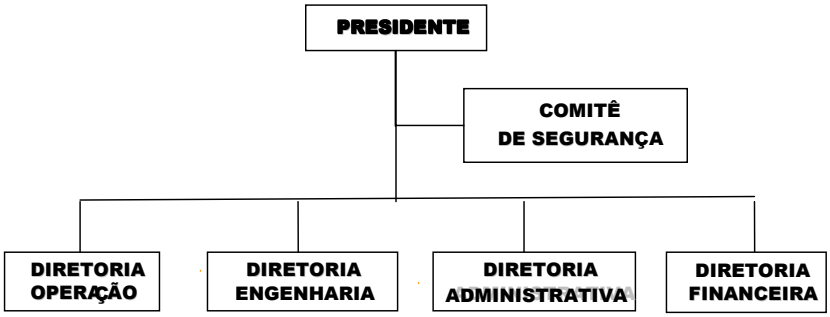

FIGURA 4: Posicionamento do Comitê Corporativo de Segurança

Este comitê deve ser formatado a partir da clara definição de seu objetivo, estrutura, funções, responsabilidades, perfil dos executores, além da formal e oficial identificação de seus membros, que darão representatividade aos departamentos mais críticos e relevantes da empresa.

O estabelecimento do Comitê de Segurança Corporativo da CHESF (CSC) deve seguir as melhores práticas em segurança da informação para empresas deste porte. Este comitê deverá ser formado pelos principais gestores da empresa (diretores, superintendentes e/ou chefes de departamento), com visões do mesmo objeto, mas de pontos distintos, sendo fundamental para a obtenção da nítida imagem dos problemas, desafios e impactos. Por isso, envolver representantes da área Tecnológica, Comunicação, Comercial, Negócios, Jurídico, Patrimonial, Financeira, Auditoria, etc., em muito agregará para o processo de gestão, de forma a evitar conflitos, desperdícios, redundâncias e o principal: fomentar a sinergia da empresa às suas diretrizes estratégicas de curto a longo prazo.

O Comitê de Segurança Corporativo é responsável pelo estabelecimento e manutenção da Política de Segurança da empresa, que servirá de base para elaboração das Instruções Normativas (IN), as quais atuarão efetivamente para garantir a segurança da informação sobre todas as camadas do MR-CITAC, bem como no relacionamento entre este e o mundo externo.

O Security Officer é o coordenador geral do Comitê Corporativo de Segurança e tem papel substancial para o sucesso do modelo, e não deve estar ligado a qualquer área da organização, com o objetivo de ser totalmente isento em suas deliberações e auditorias, como visualizado na Figura 5. É quem recebe toda a pressão da empresa diante dos resultados e quem é demandado a adequar o nível de controle, e, portanto, o nível de segurança para suprir as novas demandas do negócio. Junto ao comitê, deve mobilizar corporativamente todas as áreas associadas da empresa, deliberar medidas e contramedidas corporativas e definir índices, indicadores e metas estratégicas.

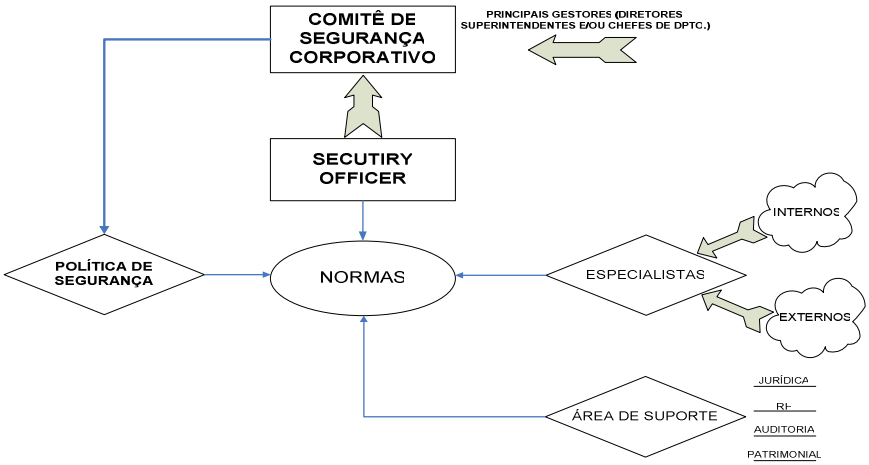

FIGURA 5: Modelagem de Interação dos Principais Elementos no Modelo de Referência

Em um segundo momento é importante a criação de Comitês Interdeparmentais de Segurança da Informação distribuídos pela empresa e localizados em departamentos ou unidades mais representativas e críticas, mantendo, em sua estrutura, atividades conforme o processo de gestão cíclico, tais como: TI, telecomunicações, Automação, Operação, Manutenção, Engenharia, RH, Administrativa, Comunicação, Compras e Contratações, e Financeira.

4.3 Perímetro de Segurança

Não há nada de novo para área de segurança, principalmente a patrimonial, em falar de perímetro. Esta estrutura de segmentação de ambientes físico é considerada estratégia militar de defesa e também se aplica ao cenário atual das empresas, mesmo que tenhamos de ultrapassar os aspectos físicos e aplicá-los para segmentar ambientes lógicos. Certamente o grande segredo para obter o melhor retorno dos mecanismos que garantem os níveis de proteção da informação está na segmentação inteligente dos ativos, ou seja, aplicar os controles adequados sem que exceda os limites e nem fique aquém das necessidades, viabilizando a efetiva redução de riscos e o aumento da segurança do negócio, sem burocracia demasiada, perda de agilidade e competitividade.

O objetivo do conceito de perímetro é enfatizar para uma determinada área, a importância da segurança da informação em seu ambiente, e definir procedimentos específicos de acordo com suas necessidades e prioridades implantando barreiras de segurança de acordo com o modelo global de gestão.

4.4 Normas Técnicas e Recomendações

A composição do modelo se baseia na internalização do conceito Governança Corporativa, prática recomendada pela Sarbanes Oxley – SOX e pelo COSO – The Comitee of Sponsoring Organizations. Para internalização desta prática, utilizam-se recomendações do ITIL (Information Technology Infrastructure Library); da norma brasileira (3) baseada na BS7799 da British Standards Institution, que deriva a BS25999 (trata do time de resposta a incidentes); das Práticas Correntes em Análise de Riscos e Gestão de Riscos; das práticas do COBIT – Control Objectives for Information and Related Technology (guia de Modelo de Referência em Gestão de TI); da Gestão de Processos (Análise de WorkFlow) e de Gerenciamento de Projetos, baseados no PMBoK do PMI.

4.5 Análise de Fronteiras

Para melhor visualização das fronteiras entre o modelo de convergência e o modelo de gestão da segurança ilustramos na Figura 6 as interações entre os modelos, ou seja: no sentido *inbound*, das camadas núcleo do para a camada periférica; e no sentido *outbound*, da camada periférica para as camadas núcleo.

5.0 - MEDIDAS DE SEGURANÇA DA INFORMAÇÃO NA CHESF

A rede de dados da CHESF possui divisão de responsabilidades quanto a sua expansão, operação e manutenção. A Superintendência de Tecnologia e Informática (STI), subordinada a Diretoria Administrativa, é responsável pelos ativos e cabling em área administrativa do complexo sede, localizado em Recife-PE. A Superintendência de Telecomunicações e Controle (STC), subordinada a Diretoria de Operação, subdividida em Departamento de

Telecomunicações (DTL) e Departamento de Proteção e Automação (DPA), é responsável pelos ativos e cabling em área operacional do complexo sede, assim como todos os ativos e cabling que dão suporte às rotinas operacionais e administrativas nos demais pontos de presença.

Considerando a existência de uma única via de interligação com a Internet através da rede local do complexo sede, percebemos que a área de TI é responsável pelo sentido outbound de interação, conforme visualizado na Figura 6, onde os possíveis ataques externos são combatidos através de "firewall", sistema de proteção de intrusão, controles de acesso, implementado na conexão da rede, complementado por atributos técnicos das estações nó da rede, para combate a ataques dos tipos DoS ou DDoS (Distributed Denial of Service).

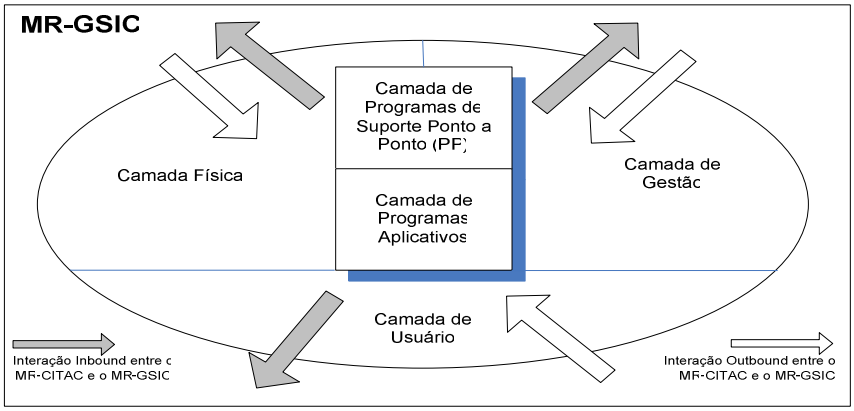

FIGURA 6: Fronteiras e Interações entre os Modelos de Referência

Nesta seção abordaremos as medidas de segurança que estão sendo tomadas no âmbito do DTL, onde estão lotados os autores deste IT, que é responsável pela rede de longa distância e redes de dados locais das diversas regionais da empresa, assim como todo o sistema de transporte associado.

Desde 2004, o DTL vem investindo na modernização da planta da rede de dados, com a substituição dos ativos núcleos do backbone, que se utilizavam de enlaces de 2Mbps e passaram a se utilizar de enlaces de 155Mbps. Nesta modernização também estão sendo substituídos as switches core, de distribuição e de borda dos diversos sites da CHESF, por ativos com funções de gerenciamento, QoS, Segurança (Criptografia e Autenticação forte) e Power over Ethernet (PoE). A expectativa é que em 2008, toda a planta esteja homogeneizada com os requisitos técnicos mínimos para operacionalização do sistema dentro da filosofia dos modelos de referência apresentados.

Diante da convergência e dos avanços tecnológicos o DTL vêm tomando medidas de segurança para adequação do seu processo às melhores práticas de Governança Corporativa tais como:

I – Estabelecimento de uma comissão formada por profissionais da camada de gestão e de usuários para elaboração da Política Corporativa de Segurança da Informação integrada e única para toda a organização.

II – Contratação de consultoria técnica especializada para análise de riscos e identificação de vulnerabilidades;

III – Participação efetiva na criação e desenvolvimento das atividades do Comitê Corporativo de Segurança, em conjunto com a STI e demais órgãos envolvidos;

IV – Ações quanto à segurança física e ambiental dos ativos de Telecomunicações:

- Consolidar a observância dos usuários à IN-TC.01.005, que trata do acesso às salas de Telecom;
- Estabelecer política para controle de acesso aos gabinetes de rede localizados na área administrativa;
- Implementar alimentação DC a todos os ativos de rede local e de longa distância, presentes em salas de equipamentos de telecom nas Subestações, Usinas e Repetidoras de Telecomunicações da CHESF;
- Fornecer alimentação através de NO-BREAKS a todos os ativos de rede que suportam servidores administrativos, e que não se encontram nas salas de telecomunicações;
- Monitorar periodicamente as instalações das Salas de Telecomunicações e gabinetes de rede local espalhados em áreas administrativas ou operacionais, verificando as condições de climatização, limpeza, possibilidade de incêndio, vazamentos d'água, além de outros riscos relacionados aos ativos;
- Disponibilizar pontos de rede de dados para acesso de usuário, em todas as salas de equipamentos de Telecom, evitando a necessidade de acesso direto nas Switches;
- Normatizar as instalações de Redes Locais Estruturadas de acordo com as normas vigentes;
- Definir procedimento para dimensionamento e manutenção do estoque mínimo de sobressalentes;
- Estabelecer política para bloqueio de portas dos ativos de rede, protegendo a rede dos acessos indevido;
- Análise de Viabilidade para montagem de Site Backup dos servidores de gerência de Telecomunicações.

V – Ações quanto ao controle de acesso aos ativos da rede de dados:

- Implementar política de configuração de senhas de usuários para as comunidades pública e privada, utilizando SNMPv2, e nos ativos que suportam SNMPv3, será utilizado o protocolo de autenticação SHA-96 e o protocolo de privacidade DES, ambos com senhas específicas;
- Desabilitar HTTP para todos os equipamentos ativos que compõem a WAN e todos os novos switches de borda. Os demais switches poderão ter o HTTP habilitado, com usuário e senhas específicos;
- Habilitar FTP nos equipamentos de rede, onde os usuários utilizarão a mesma senha e usuário de Telnet, o usuário Anônimo será banido;
- Para acesso via TELNET, habilitar os usuários User (somente leitura) e Manager (Leitura e escrita), ambos com senhas específicas. O protocolo SSH será habilitado sempre que possível;
- Quanto à política de senhas, as senhas serão, em geral, de oito dígitos, com letras e números. Serão renovadas a cada seis meses, ou em casos excepcionais, a ser definido pelo órgão normativo.

VI – Para as diversas aplicações, que apresentam níveis de comprometo distintos dos fatores que influenciam na Qualidade de Serviço (QoS), está sendo iniciado pela camada de gestão, melhorias, atualizações e substituição de aplicativos, configuração das tabelas de roteamento, estabelecimento do nível de prioridade (Diffserv) entre as aplicações, o “Policiamento de Tráfego”, para garantir o grau de satisfação estabelecido junto a camada de usuário. Em conjunto com estas ações está sendo implementada uma politica de utilização de aplicativos.

VI – Segmentação da rede por VLAN, utilizando prioritariamente duas divisões: Operacional e Corporativa.

6.0 - CONCLUSÕES

A segurança é aplicada há várias décadas nas mais diversas atividades e com os mais diversos propósitos. O ano de 2006 foi agitado e os investimentos na área foi expressivo na maioria das grandes empresas, sendo direcionados por dois fatores: atendimento a regulamentações e reação a incidentes internos ou externos.

A CHESF possui cada vez mais uma rede integrada, por onde trafegam informações operacionais e administrativas. Sua organização interna considera diferentes órgãos para gestão das áreas de telecomunicações, automação e controle, e TI, tornando a implementação da segurança da informação um grande desafio, cujo sucesso depende da integração dos diversos órgãos. Por isso as ações precisam estar intimamente alinhadas às diretrizes estratégicas da empresa e, para isso, é necessário ter uma visão corporativa, global e ampla, capaz de criar sinergia entre as atividades e, principalmente, maior retorno sobre o investimento. Este último, conseguido principalmente pela eliminação de ações redundantes e, muitas vezes conflitantes, que depreciam o plano corporativo de segurança da informação.

Para o sucesso deste modelo é fundamental que o comitê corporativo esteja posicionado em um nível hierárquico com autonomia, integrando com os aspectos tecnológicos, físicos e humanos, e que a empresa esteja sempre em um processo cíclico e contínuo de gestão de segurança da informação preparado para as variáveis que interferem direta e indiretamente nos riscos operacionais do negócio, ou seja, mudanças mercadológicas, inovações tecnológicas, expansão física e humana , etc., que acabam mexendo na equação do risco.

7.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) Peló, D. U., Desenhando nossa Infra-Estrutura de Rede para a Convergência, XVIII Seminário Nacional de Produção e Transmissão de Energia Elétrica - SNPTEE, Florianópolis, 2005.

(2) Sêmola, M., Gestão da Segurança da Informação: Uma Visão Executiva, Elsevier Editora Ltda., 2003.

(3) Associação Brasileira de Normas Técnicas. Tecnologia da Informação: Código de Prática para Gestão da Segurança de Informações - NBR 17799. Brasil.

(4) Prescott, R., Revista InformationWeek Brasil, Ano 8, No. 174, Janeiro de 2007.

8.0 - DADOS BIOGRÁFICOS

Rodrigo Leal de Siqueira, nasceu em Recife em 1977, graduado em Engenharia Eletrônica pela UFPE em 2000. Concluiu o Mestrado em Engenharia Elétrica, com ênfase em Telecomunicações, em 2004 pela mesma instituição. Atualmente está cursando MBA em Gerência de Projetos pela Fundação Getúlio Vargas e é Engenheiro da Divisão de Engenharia e Expansão do Sistema de Telecomunicações da CHESF, desde 2006. Durante o período de 2000 a 2006 foi Gerente de Projetos na área de Telecomunicações em uma empresa de Consultoria, atuando principalmente na área de implantação. Publicou artigo técnico no IEEE Vehicular Technology Conference 2006 em Melbourne na Austrália e no Simpósio Brasileiro de Telecomunicações em 2005 no Rio de Janeiro no Brasil.

Alexandre Wagner D. Lira, nasceu em Natal em 1976, graduado em Engenharia Eletrônica pela UFRN em 2002. Pós-Graduado em Gerência de Projetos pela Faculdade Santa Maria em 2007. Engenheiro da Divisão de Engenharia e Expansão do Sistema de Telecomunicações da CHESF, desde 2002. Publicou artigo técnico na área de telecomunicações no IMOC 2001 em Belém e no SBPC 2000, em Brasília no Brasil.