SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

GTL 13
14 a 17 Outubro de 2007
Rio de Janeiro - RJ

GRUPO XVI

GRUPO DE ESTUDO DE SISTEMAS DE INFORMAÇÃO E TELECOMUNICAÇÕES PARA SISTEMAS ELÉTRICOS – GTL

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SOX EM UMA REDE DE DADOS INTEGRADA. DIVISÃO DE RESPONSABILIDADES NA CHESF

Elton Bernardo Bandeira de Melo *

COMPANHIA HIDRO ELÉTRICA DO SÃO FRANCISCO - CHESF

RESUMO

A segurança da informação tem ocupado cada vez maior papel de destaque nas estratégias de gestão empresarial. A implementação de uma política de segurança da Informação eficaz em uma empresa do setor elétrico, mostra-se uma tarefa bastante desafiadora e complexa. Na CHESF esta complexidade é aumentada devido à plataforma integrada de dados, por onde trafegam informações operacionais e administrativas simultaneamente, e pela necessidade de adequação à legislação Sarbanes-Oxley (SOX), conforme diretriz da Eletrobrás. Este trabalho tem como objetivo analisar este contexto, apontando as iniciativas adotadas pela empresa e suas perspectivas.

PALAVRAS-CHAVE

Segurança da Informação, Sarbanes-Oxley, Rede de dados Integrada

1.0 INTRODUÇÃO

A segurança da informação já é atualmente reconhecida como vital dentre as empresas. São assustadoramente crescentes os investimentos realizados na aquisição de ferramentas para implementação de segurança de dados, na modificação de processos, auditorias e consultorias especializadas para que este precioso ativo intangível esteja a salvo contra ataques, acidentes, negligência ou uso indevido. De fato, o manejo indevido de informações estratégicas pode levar à perda de competitividade, fraudes, perdas de oportunidades, de recursos materiais, de capital e até descontinuidade dos negócios, e assim arruinar qualquer possibilidade de sucesso empresarial. Esta relevância é aumentada quando se trata de empresas de tecnologia intensiva, tal como empresas de energia, devido ao alto requinte dos processos, à suprema importância do planejamento estratégico, aos montantes de capital envolvidos nas manobras financeiras e na importância da pesquisa e desenvolvimento, que garantam através da inovação aumento da competitividade, e conseqüente sucesso corporativo.

Em 2003, a diretoria da Eletrobrás publicou a decisão de adequar todas as suas subsidiárias, dentre as quais se encontra a CHESF, à legislação Sarbanes-Oxley (SOX) (1). Sua implementação está alinhada com a necessidade das companhias mostrarem transparência quanto aos seus processos contábeis, bem como dos sistemas de informação que apóiam estes processos, de modo que recai na implementação de Segurança de Tecnologia da Informação (TI) uma maior responsabilidade, pois a não implementação de algumas práticas pode implicar na inadequação à lei.

Nas empresas do setor elétrico, além dos possíveis requisitos imputados pela SOX, a implementação eficaz de uma política corporativa de segurança da informação requer um enorme esforço por parte dos mais diversos segmentos internos, como os departamentos financeiros, contábeis, de TI, telecomunicações, automação e

(*)Rua Delmiro Gouveia, 333 – Anexo 2 – Sala 117 - CEP 50761-901 - Recife - PE - BRASIL
Tel.: (081) 3229-4295 - Fax: (081) 3229-4217 - e-mail: eltonbm@chesf.gov.br

controle da planta elétrica, recursos humanos, etc., e principalmente da alta direção. Requer ainda uma forte integração entre estas áreas, formação de comitês específicos para tratarem o tema, ferramentas avançadas de proteção e análise, suporte externo especializado e um grande empenho na conscientização dos colaboradores. O que torna a missão deveras difícil, requerendo pois, um exaustivo planejamento.

Este trabalho tem como objetivo elucidar as questões relacionadas à implementação de uma política de segurança da informação na CHESF, considerando as peculiaridades das empresas do setor elétrico (seção 2), os impactos acarretados pela SOX (seção 3), algumas necessidades para as implementações de uma política de segurança eficaz (seção 4) e as características da plataforma de telecomunicações e dos sistemas de informação presentes na CHESF, além de apontar os principais traços da necessária atribuição de responsabilidades entre os órgãos que compõem a companhia (seção 5). Os aspectos técnicos relacionados à implementação da segurança da informação, tais como os protocolos utilizados, a disposição e a configuração dos equipamentos de adquiridos, não serão tratados neste trabalho.

2.0 ASPECTOS DE SEGURANÇA DA INFORMAÇÃO ESPECÍFICOS DO SETOR ELÉTRICO

Além dos riscos inerentes às falhas humanas ou dos equipamentos, na operação dos sistemas, as empresas de energia, como provedoras de serviços essenciais ao funcionamento adequado da sociedade (muitas vezes até indispensáveis à sobrevivência humana), podem se tornar alvos de atentados de organizações contrárias a esta organização social, ou de indivíduos intencionados em mostrar suas habilidades computacionais através de invasões eletrônicas, os chamados *hackers.* Estes aspectos reforçam a necessidade de implementação de políticas rígidas de segurança nestas empresas. No sentido de estabelecer um conjunto de princípios para o tratamento da segurança da informação no setor elétrico, um grupo de estudo conjunto do *Cigré* foi montado em 2003, o *JWG D2/B3/C2-01,* cujos trabalhos (2)(3) de conclusão forneceram muitos subsídios a esta seção, ali alguns relatos de incidentes de possíveis ataques *hackers* às empresas de energia são descritos. Seguindo o documento supracitado, utilizaremos o termo “segurança cibernética”, como sendo aquela relacionada às informações que podem interferir na operação de equipamentos de controle, proteção, supervisão e automação elétrica.

Computadores estão presentes em todos os níveis de negócio em uma empresa de energia elétrica, desde o controle da rotação das máquinas geradoras até o computador portátil utilizado pelo gerente de finanças. As decisões de quais informações devem ser protegidas passa por uma análise de riscos minuciosa, tendo em vista a relação custo-benefício de cada par risco-solução para a avaliação dos potenciais prejuízos pelo não estabelecimento de uma determinada facilidade de segurança em um dado ativo, sistema ou processo.

Não obstante a alta dependência computacional em todos os negócios inerentes às empresas de energia, uma forte tendência à integração dos diversos sistemas torna o aspecto da segurança ainda mais delicado e difícil. No início da digitalização dos sistemas de controle, proteção e automação das subestações e usinas, os computadores utilizados pelos funcionários para as tarefas administrativas, tais como acessos aos sistemas de gestão de pessoal, financeiro ou Intranet estavam em máquinas separadas. Com a gradativa convergência dos protocolos de comunicações industriais para a plataforma TCP/IP, há uma tendência, já percebida em diversas empresas, à plena integração entre redes operacionais e administrativas. Com isto, através do mesmo equipamento e da mesma interface de comunicação, trafegam simultaneamente dados dos aplicativos operacionais, tais como SCADA/EMS (Sistema supervisório e de aquisição de dados/ Sistema de Gerenciamento de Energia), Intranet e até Internet. Esta integração traz consigo diversas vantagens, conforme discutiremos mais adiante, mas também acarreta uma maior dificuldade na proposição de uma solução eficaz para a segurança da informação.

2.1 Integração das Redes Corporativas

A evolução das telecomunicações e de TI, juntamente com a convergência dos protocolos de comunicação e o modelo TCP/IP possibilitaram às empresas de energia, a construção de uma plataforma integrada de comunicação. Apesar disso, diversas empresas optaram por manter seus sistemas operacionais e administrativos, separados, i.e., uma rede operacional, conectada ao sistema SCADA/EMS e aos terminais de acesso, e uma rede corporativa administrativa, projetada para suprir as necessidades de aplicações tais como Internet, Intranet, e-mail, e demais sistemas administrativos. Nestas empresas, computadores estão dedicados àpenas uma das redes. Ali, prevalece o argumento de que segurança e confiabilidade devem ser reforçadas no ambiente operacional, no entanto há diversos pontos que contam contra este tipo de segmentação tais como:

a. Em uma rede de pacotes, quanto maior o número de roteadores interconectados, maior é o número de rotas alternativas entre dois possíveis pontos, de modo que, a resiliência das redes isoladas (administrativa e operacional) é menor que a resiliência das redes interligadas;
b. Em muitas localidades é necessário uma duplicação de *hardware* (dois roteadores, dois canais de comunicação, dois computadores, etc.), acarretando um custo elevado;
c. São necessárias duas políticas de segurança, o que inclui, anti-vírus, auditorias, listas de acesso, *firewall*, etc., isto acarreta um aumento nos custos e maiores chances de falhas humanas;

d. Maior dificuldade de conscientização dos colaboradores para não utilizarem os mesmos equipamentos (que devem ser semelhantes) para finalidades operacionais e administrativas, apesar das possível perda de produtividade;
e. Algumas aplicações administrativas são essenciais ao negócio da empresa, tal como o sistema de abertura de Ordens de Serviço de Manutenção, Solicitações de intervenções, Gerência de ativos, Leilões eletrônicos, etc., o que impõe caráter crítico à rede administrativa em termos de disponibilidade, confidencialidade, etc.

Contudo, há um ponto que pesa contra a integração das redes: o número de pontos de acesso às redes administrativas é bem mais elevado, o que aumentaria a vulnerabilidade de uma rede integrada, exigindo um maior investimento em ferramentas de controle da segurança e uma política única de segurança para todos segmentos da empresa.

2.1 Domínios de Segurança

Devido à alta integração das redes corporativas, inclusive entre os setores administrativos e operacionais, surgiram diversas dificuldades para se analisar, descrever ou classificar uma rede de computadores através de suas características de *hardware*, tais como roteadores, *switches*, ou servidores. Uma abordagem alternativa se dá pela definição dos Domínios de Segurança.

Um Domínio de Segurança é uma área específica, onde as operações de atividades/negócios específicas estão em andamento e podem ser agrupados. O objetivo do conceito de domínio é enfatizar para os envolvidos em uma determinada área, a importância da segurança da informação em seu ambiente, e definir procedimentos específicos de acordo com suas necessidades. Exemplos de domínios de segurança são: subestações, telecomunicações, TI, Operação de tempo-real, usinas, etc.

Não existe, no entanto, um modelo para a definição dos domínios de segurança dentro de uma determinada empresa ou região, tampouco há um procedimento bem estabelecido para realizar a avaliação de riscos em tais domínios. Soluções particulares para cada domínio de segurança podem desenvolvidas separadamente, no entanto, se os domínios são interligados, furos do esquema de segurança de um podem levar a falhas em ambos, de modo que a composição isolada de uma política de segurança não se mostra um caminho eficaz nestes casos. Um estudo dentro de cada domínio de segurança permitiria mapear as relações inter ou intradomínio e definir as características de cada domínio, tais como autoridade, perímetro, níveis de segurança e políticas para a interconexão de domínios. As formalizações das relações interdomínios podem ser feitas, por exemplo, através de SLAs (Service Level Agreements) específicos que designem os responsáveis pela segurança das informações na conexão.

2.2 Controle Supervisório, Aquisição de dados e Gerenciamento de Energia (SCADA/EMS)

O gerenciamento dos equipamentos de potência do setor elétrico, tais como transformadores e linhas de transmissão, estão cada vez mais expostos às ferramentas de proteção, controle e automação digitais, configuradas através de *software* presentes em *notebooks* ou *PCs*. Muitas vezes estas configurações são realizadas remotamente, utilizando protocolos de comunicação proprietários, ou mesmo padrões, como o SNMP (*Simple Network Management Protocol*). A configuração de um relé de proteção pode ser feita a quilômetros de distância por um usuário não autorizado, caso este consiga as chaves de acesso ao equipamento, e o mesmo esteja conectado à plataforma integrada de comunicação corporativa, que por sua vez, toca a Internet. Com isto, cada vez mais os ativos de grande porte do setor elétrico, responsáveis pela produção ou transmissão de energia, estão mais expostos a ataques maliciosos e ao uso indevido dos recursos de TI e telecomunicações (vírus presentes um terminal de acesso, seria um outro exemplo).

Uma breve análise de um sistema SCADA típico revela uma enorme quantidade de vulnerabilidades, como múltiplos pontos de acesso dispostos ao longo de diferentes sistemas de TI, e até plataformas contratadas das operadoras de telecomunicações, por onde trafegam dados operacionais vitais aos negócios do setor elétrico. Os fabricantes dos sistemas SCADA/EMS têm a necessidade de estabelecer padrões de protocolos para que seja possível assegurar a segurança das informações manipuladas pelos diversos agentes do setor, mas não há ainda um conjunto de protocolos que permita tal implementação. Ademais, há uma tendência de cada vez mais sistemas operacionais, como por exemplo teleproteção, convergirem para protocolos suportados nas plataformas TCP/IP, uma vez que já há tecnologia para sistemas de tempo real e que requerem alta Qualidade de Serviço (QoS) (4).

2.3 Diretrizes gerais para a Segurança da Informação nas Empresas de energia Elétrica

Como principais recomendações às empresas de energia elétrica, tendo em vista todas as limitações tecnológicas e as inevitáveis tendências de convergência dos protocolos de comunicação, além dos procedimentos gerais (seção 4), poderiam ser listadas as seguintes medidas para uma estratégia de segurança cibernética:

a. Definir responsabilidades e autoridades pela segurança da informação em cada domínio de segurança;
b. Documentar toda a arquitetura de rede e identificar os sistemas de tempo real;
c. Realizar auditorias de segurança em todos os sistemas interconectados e de tempo real;

d. Identificar todas conexões aos sistemas de tempo real;
e. Retirar conexões e aplicativos desnecessários dos sistemas de tempo real;
f. Fortalecer o controle de acesso aos sistemas remanescentes;
g. Instalar facilidades de segurança propostas pelos fornecedores especializados;
h. Estabelecer critérios de controle sobre os acessos não rotineiros;
i. Preparar um processo compreensível e contínuo de gerência de riscos;
j. Implementar *firewalls* e sistemas de detecção e prevenção de intrusos *IDS/IPS*;
k. Avaliar a integridade física dos sistemas de tempo real;
l. Estabelecer uma filosofia de segurança cibernética organizacional, e;
m. Estabelecer um sistema de procedimentos de *backup* e planos para recuperação de disastres.

3.0 IMPACTOS DA LEI SARBANNES-OXLEY

A lei Sarbanes-Oxley (SOX) (1) instituída em 2002, provê novas regras de governança corporativa regulamentações e padrões para as empresas que querem ser registradas na Comissão de Valores Mobiliários (CVM) dos E.U.A. (*Securities and Exchange Comission – SEC)*, ou seja, aquelas que têm capital aberto com ações na bolsa americana ou negociações na Nasdaq. A SOX estabelece um arcabouço para os controles internos destas empresas a fim de evitar novos escândalos por fraudes por manipulações das informações financeiras, como os que envolveram as empresas *Enrom*, *Tyco* e *WorldCom*. A premissa básica é que uma boa governança corporativa e práticas éticas nos negócios não são de maneira alguma, refinamentos opcionais. São obrigações corporativas e são de responsabilidade dos executivos do alto escalão das empresas. Embora haja muitas seções na Lei, para estabelecer tal arcabouço, três seções em particular tocam a área de TI:

- **Seção 302 - Estabelece responsabilidades corporativas pelos relatórios financeiros:** Em linhas gerais, requer dos diretores executivos e financeiros das empresas, a responsabilidade pela certificação, revisão, integridade, clareza e completeza dos relatórios financeiros e contábeis trimestrais e anuais das empresas. Além da avaliação periódica da eficácia dos controles internos, de modo que imputa aos executivos a responsabilidade por todas e quaisquer informações financeiras declaradas publicamente. Tais diretores são responsáveis por informar à comissão de auditores, todas as deficiências no projeto ou alteração dos controles internos que possam impactar na captação, armazenamento ou divulgação dos dados financeiros. Todas as insuficiências materiais nestes controles internos também devem ser identificadas e informadas ao comitê auditor.
- **Seção 404 - Estabelece o gerenciamento da avaliação dos controles internos:** os relatórios anuais devem conter uma seção sobre os controles internos, indicando responsabilidade pelo gerenciamento e manutenção adequados de uma estrutura de controles internos eficazes e procedimentos para a emissão de relatórios financeiros. As empresas devem declarar que os relatórios financeiros foram auditados e atestados por uma comissão externa.
- **Seção 409 - Trata da divulgação das informações em tempo real:** cada emissor, submetendo relatórios financeiros, deverá divulgar ao público em base rápida e corrente tal informação adicional com respeito a mudanças materiais na condição financeira ou operacional do emissor, em linguagem simples e que deve incluir tendências, informações qualitativas e apresentações gráficas, conforme a SEC determina como regulamentação. É necessária e útil para a proteção de investidores e no interesse público. Esta seção apresenta uma forte tendência de impactos maiores em longo prazo, quando as necessidades de mercado de informação moderno, aliada ao uso de novas tecnologias computacionais, irão tornar o uso desta provisão como uma alavanca para finalmente chegar à divulgação em tempo real das informações financeiras, e até divulgação de contratos e compromissos em processo, mesmo antes de sua realização contábil tradicional.

Há a noção por parte dos administradores, de que a confiabilidade dos relatórios financeiros é fortemente dependente de um ambiente de TI bem controlado, de modo que há uma tendência das organizações considerarem os controles TI no contexto dos controles dos relatórios financeiros. Fica claro, no entanto, que apenas os Sistemas de Informações e infra-estrutura de TI que envolvem os relatórios financeiros estão submetidos às exigências da SOX. Aspectos de TI relacionados aos controles operacionais e aos aspectos de eficiência das empresas não estão aí inseridos, embora haja uma tendência desejável de que controles semelhantes sejam entendidos às demais áreas das empresas, incluindo a operacional.

3.1 Em busca da adequação aos requisitos da SOX nas empresas do Setor Elétrico

De fato, a responsabilidade do segmento de TI no processo de adequação aos requisitos da SOX são tremendas, pois em todas as empresas, a aquisição de dados contábeis e financeiros, o armazenamento destes dados e a emissão dos relatórios financeiros que posteriormente serão tornados públicos dependem fortemente de uma estrutura de TI controlada. Tais controles não são de fácil implementação, requerem executivos de TI capacitados para estas tarefas, uma avaliação de riscos criteriosa, documentação dos processos, indicação de responsáveis, monitoramento e controle do ambiente de TI, além de ferramentas apropriadas para a implementação de segurança. A documentação disponível sobre a adequação à SOX e os arcabouços de TI necessários são

extensos. As principais definições neste sentido, vêem do COSO (Comitee of Sponsoring Organizations of the Treadway Comission), uma organização privada, voluntária, dedicada à melhoria da qualidade dos relatórios financeiros através da postura ética nos negócios, formada em 1985.

Em empresas do setor elétrico, onde a plataforma de TI é distribuida ao longo da empresa, é natural que haja uma restrição da Política de Segurança da Informação conseqüente da implementação da SOX à área de influência sobre os relatórios financeiros. De fato há uma certa liberdade na legislação para que as empresas declarem o escopo de TI sob controle passível de auditoria para adequação à SOX. Fica claro então que um domínio de segurança restrito às aplicações e infra-estrutura que impactem nos relatórios financeiros deve ser definido, um conjunto de procedimentos de controle específicos devem ser aplicados a este domínio, seguindo o arcabouço definido pelo COSO. Conforme dito anteriormente, caso as ferramentas de controle sejam extensíveis a outros domínios de segurança, não há porque não fazê-lo, tendo em vista a melhoria dos processos internos. O que não deve acontecer é a submissão destas áreas, muitas vezes operacionais, aos rígidos controles impostos e seus custos associados, sob o argumento de adequação da empresa à SOX. No grupo Eletrobrás, dois grupos de trabalhos foram definidos em para lidar com adequação dos recursos de TI:

- TICA – Responsável pelo controle dos sistemas de informação submetidos à adequação à SOX, e;
- TIGC – Responsável pela infra-estrutura de TI que suporta os aplicativos mapeados pelo TICA;

Nenhuma aplicação operacional é mapeada pelo TICA, de modo que a definição do domínio de segurança sob égide do TIGC é também restrita ao ambiente que envolve relatórios financeiros.

4.0 IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Freqüentemente, devido ao grande porte das empresas que compõem o setor elétrico junto à evolução histórica dos segmentos organizacionais presentes nestas empresas, vê-se que há uma separação típica entre órgãos de diferentes características:

a. Responsáveis pelos sistemas de informações corporativos não operacionais, ou seja, aqueles que não interferem diretamente nos equipamentos responsáveis pela produção e transmissão de energia, estes são geralmente compostos por bachareis em ciência da computação, analistas de sistemas e programadores, contando com uma pequena parcela de analistas de redes;
b. Os responsáveis pelos sistemas SCADA/EMS, geralmente composto por engenheiros eletrônicos, eletrotécnicos e técnicos eletricistas. Este segmento organizacional está, em geral, mais ligado à operação do setor elétrico, pois seus trabalhos de parametrização de relés, configurações de IHMs e outras ferramentas para aquisição de dados;
c. Os responsáveis pelas telecomunicações, que, em empresas que possuem uma plataforma privada de comunicações, envolve em sua maioria técnicos e engenheiros de telecomunicações, provendo, planejando, construindo, gerenciando e mantendo estas redes. São responsáveis pelos meios físicos de transmissão, tais como fibras ópticas, enlaces de rádio, cabos coaxiais, cabos UTP, etc., pelas configurações das centrais telefônicas, *switches*, roteadores e demais componentes que servem de suporte ao serviços IP.

Estes grupos definem claramente domínios de segurança diferentes, e, corroborando o exposto na seção 2.1, esforços individuais na implementação de segurança quando os domínios estão interligados, podem estar fadados ao fracasso. Isto sugere a composição de uma Política da Informação integrada. As normas ISO/IEC 17799:2000(E) e ISO/IEC FDIS 27001:2005(E) (5) (6), que descrevem um Código de Prática para Gestão da Segurança de Informações, fornecem alguns pontos merecem destaque no contexto das empresas do setor elétrico, ou mais especificamente da CHESF.

4.1 Objetivo da Política da Informação

Fornecer direção e apoio gerencial para a segurança de informações. A gerência deve estabelecer uma direção clara e demonstrar suporte e comprometimento com, a segurança das informações através da emissão e manutenção de uma política de segurança de informações para toda a organização.

As diferenças relacionadas anteriormente entre grupos de segmentos diferentes de uma empresa do setor elétrico reiteram a necessidade de participação da direção para proporcionar uma melhor integração entre as áreas e possibilitar a construção de uma política eficaz. Pois tais diferenças muitas vezes têm fortes impactos no momento da implementação de uma política de segurança da informação, criando uma tendência às iniciativas isoladas dentro de cada grupo, procedimentos heterogêneos e perda do foco. As responsabilidades pela proteção de ativos individuais e pela condução de processos de segurança específicos devem ser claramente definidas. Reafirmando as necessidades trazidas pela SOX.

4.2 Fórum interfuncional para coordenação da Política de Segurança

Segurança de informações é uma responsabilidade corporativa compartilhada por todos os membros da equipe

gerencial. Portanto, deve ser considerada a construção de um fórum gerencial para assegurar a existência de direção clara e suporte visível por parte da gerência para as iniciativas de segurança. Esse fórum deve promover a segurança dentro da organização através de comprometimento apropriado e alocação de recursos adequados. Em uma organização de grande porte, como no caso da CHESF, é necessário um comitê interfuncional de representantes das gerências dos setores relevantes da organização para coordenar a implementação de controles de segurança da informação. No caso de haver segmentos com os perfis acima relacionados, o fórum gerencial multifuncional, ou comitê multidisciplinar de segurança da informação deverá conter representações de cada grupo, além de outros representantes relevantes, como por exemplo do setor contábil e financeiro.

4.3 Melhores práticas na implementação de uma Política de Segurança da Informação

A experiência tem mostrado que os fatores seguintes freqüentemente são críticos para a implementação bem-sucedida da segurança de informações dentro de uma organização:

a. Política, objetivos e atividades de segurança que reflitam os objetivos do negócio – embora cada segmento isolado tenha contribuições indispensáveis para o sucesso da corporação, o foco das implementações de segurança deve ser único e integrado;
b. Uma abordagem para implementar a segurança que seja consistente com a cultura organizacional – respeitar os tempos necessários às mudanças culturais, procurar tornar transparente para os usuários finais, o maior número de procedimentos de segurança possível;
c. Suporte visível e compromisso por parte da administração – é crucial a demonstração de interesse nas políticas de segurança da informação por parte da direção das empresas;
d. Um bom entendimento das necessidades de segurança, avaliação e gerenciamento de riscos – Trata-se de uma das tarefas mais complexas no processo de implantação de um Política. Esta etapa é indispensável para estabelecer quais riscos organizacionais merecem os maiores investimentos, evitando também o desperdício de recursos com sistemas superdimensionados ou a vulnerabilidade por negligência;
e. Marketing de segurança eficaz para todos os gerentes e empregados – os maiores índices de incidentes de segurança ocorrem por atuação de pessoal interno desavisado ou mal intencionado, o Marketing é fundamental para assegurar melhores índices de desempenho da política adotada;
f. Distribuição de orientação sobre a política e os padrões de segurança de informação para todos os empregados e contratados;
g. Fornecimento de treinamento e educação apropriados;
h. Um sistema abrangente e balanceado de medição, usado para avaliar o desempenho na gestão de segurança de informações e sugestões de feedback para melhorias - Ciclo PDCA (P*lan – Do – Check – Act*);

As responsabilidades locais pelos ativos físicos individuais e ativos de informação e processos de segurança, tais como o planejamento da continuidade do negócio, devem ser claramente definidas. Neste caso há uma tendência a se respeitar os domínios de segurança, e fica patente a necessidade de interação sinérgica entre os reponsáveis por cada domínio na tentativa de estabelecer um plano de continuidade do negócio global da empresa. Muitas outras diretrizes são apresentadas nas normas acima citadas, e muitas destas merecem uma análise contextualizada às empresas do setor elétrico, de modo a tentar estabelecer padrões para a elaboração de uma política eficaz. Hoje, no entanto, a depender do nível de detalhamento requerido, tais padrões inexistem.

5.0 DIVISÃO DE RESPONSABILIDADES NA CHESF

A construção de uma Política de segurança da Informação integrada, capaz de atender às demandas da CHESF, requer um enorme empenho por parte de diversos segmentos ao longo da estrutura organizacional, além do comprometimento por parte da direção e presidência, conforme explicitam as principais normas e padrões para este tipo de processo, referenciado na seção 4. Em uma empresa do porte da CHESF, já seria de se esperar que vários aspectos relacionados à proteção da informação estivessem contemplados. De fato, iniciativas isoladas, principalmente dos segmentos de TI e de telecomunicações, têm trazido à empresa ações para a mitigação dos riscos envolvendo a segurança das informações e a consciência da importância da construção de uma política integrada, com respaldo da alta hierarquia. Há uma forte sobreposição de competências e responsabilidades entre estes dois segmentos, devido à convergência das plataformas de comunicação das redes IP. Este é outro ponto que pesa a favor da construção de um comitê multifuncional para a coordenação da Política.

5.1 Estrutura da CHESF e Plataforma TCP/IP integrada

A grosso modo, a CHESF é composta por uma presidência (PR) e quatro diretorias: administrativa (DA), financeira (DF), de engenharia (DE) e de operações (DO), todas são, à sua maneira, clientes da rede TCP/IP. No tocante à elaboração e manutenção de uma política de segurança da informação integrada, à superintendência de tecnologia da informação (STI) e à superintendência de telecomunicações, automação e controle (STC), cabem as maiores responsabilidades, pois aí estão contemplados os departamentos responsáveis pelos sistemas de informações (DSI) e (DSA), pela infra-estrutura de redes, pela plataforma de telecomunicações (DTL), e pelas áreas de automação, proteção e controle dos equipamentos elétricos (DPA). O Departamento de Riscos (DPR),

dentro da superintendência de controle e execução financeira (SEF) é responsável pela gerência de riscos na empresa e, como visto anteriormente, tende a desempenhar um importante papel na elaboração da Política de Seguraná da Informação.

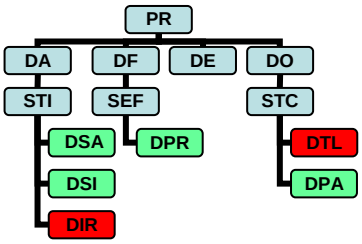

Figura 1 – Organograma resumido da CHESF

De outro modo, a CHESF pode ser dividida entre SEDE, localizada no Recife e Gerências Regionais Leste (GRL), Oeste (GRO), Paulo Afonso (GRP), Norte (GRN) e Sul (GRS), localizadas respectivamente em Recife, Teresina Salvador, Paulo Afonso, Fortaleza, e Sobradinho. A sede comporta todos os órgãos normativos e a maior parte da empresa, enquanto as regionais possuem suas sedes administrativas e suportam as equipes executivas que lotam as subestações e usinas. Cada uma destas localidades (cerca de 110) possui uma rede local de computadores, LAN(*Local Area Network*), com aplicações administrativas e operacionais, as diversas LANs estão interligadas através de uma rede maior, de longa distância WAN (*Wide Area Network).* A LAN da sede e da GRL são de responsabilidade do DIR, enquanto a WAN e LANs das demais gerências e todas as subestações e usinas são de responsabilidade do DTL. (Figura 2-a).

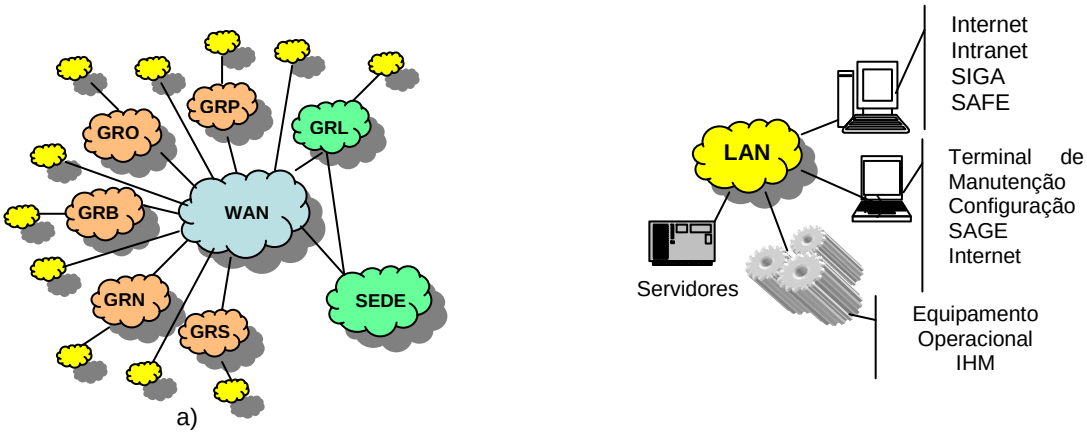

Figura 1 – Rede de dados integrada da CHESF: a) Redes interligadas e; b) Aplicações compartilham mesma rede.

Na CHESF não existe segmentação entre rede operacional e rede administrativa, a rede é única e integrada, e por ela trafegam todos os dados da empresa, desde SAGE (Sistema Aberto de Gerenciamento de Energia, Medição de faturamento, até leilões eletrônicos e internet)(Figura 2-b). As redes sob responsabilidade do DTL e DIR estão interconectadas no Recife em vários pontos, trocam pacotes de controle, roteamento, e desta forma, possuem uma interdependência no tocante à segurança da informação. Fica claro aqui que, não adiantaria fortalecer a política de segurança em um dos lados se o outro não estiver em sincronia, pois, o dano será comum e, em geral, se dará pelo lado menos fortalecido. Apesar disso, não existe ainda um pleno nivelamento das medidas de segurança entre os dois departamentos.O DTL instituiu um grupo de trabalho para lidar com o tema da segurança da informação nos aplicativos sob sua responsabilidade. Este grupo vem tomando iniciativas para suprir carências latentes relacionadas ao tema, tais como a definição de uma política de senhas de configuração dos roteadores e *switches*, controle do acesso físico às instalações, aumento da disponibilidade, implementação de QoS, controle de acessos etc. Do outro lado, o DIR tem iniciativas e motivações distintas, embora muitas vezes compatíveis. Isto se dá por não haver uma norma supra-departamental que imponha o mesmo padrão a ambos.

5.2 Pesquisa e Desenvolvimento

Tendo em vista a ausência de padrões bem estabelecidos para o tratamento do tema da segurança da informação dentre as empresasd do setor elétrico, conforme discutido na seção 2, faz-se necessário um trabalho de pesquisa e desenvolvimento (P&D) nesta área, de modo que as peculiaridade destas empresas sejam melhor compreedidas, estruturadas e assim, aumente-se as chances de uma segurança da informação mais eficaz. Os engenheiros da CHESF enxergaram esta necessidade e vêm propondo projetos de pesquisa em temas complementares. Foram propostos e aprovados três projetos de P&D relacionados ao tema.

- Metodologia para uma WAN ótima à Chesf (DTL);
- Segurança da Informação na rede de controle e automação (DPA), e;
- Metodologia de Dimensionamento e Identificação de Modelo de Suporte à Qualidade de Serviço (QoS) em redes IP com tecnologias DIFFSERV/MPLS (DIR);

Isto mostra a atenção que os temas relacionados à correta gestão dos ativos de TIC vêm tomando dentre os especialistas da área. Por outro lado, enfatiza a necessidade integração entre as áreas de telecomunicações, controle e automação e infra-estrutura de redes, cada uma responsável por um dos projetos, respectivamente.

5.3 A SOX na CHESF

Os resultados dos trabalhos de adequação da CHESF aos requisitos da SOX, resultaram em várias melhorias nos processos internos de controle. Podemos relatar como frutos da adequação à SOX:

- O TICA mapeou e adequou os controles de 38 processos de negócio da empresa, suportados por 21 sistemas de informações (todos relacionados aos relatórios financeiros, nenhum operacional);
- O TIGC mapeou e adequou 6 processos para dar suporte aos 21 sistemas citados acima, sendo que alguns destes processos resultaram em Instruções Normativas, algumas relacionada à segurança no domínio de segurança que envolve os relatórios financeiros.

Além destas ações, o advento da SOX serviu para atentar para a necessidade de consultoria externa especializada nesta área, para a motivação à aquisição de ferramentas de análise de vulnerabilidades e para convencer a Diretoria Administrativa da necessidade de um plano de continuidade dos negócios de TI, programada para o ano de 2007. Vê-se que, de certa forma SOX teve impactos positivos na consolidação de uma ambiente de governança de TI melhor controlado e com vistas à questão da segurança.

5.4 Formação de comitê multidisciplinar

A criação de um departamento formal dentro da diretoria financeira da CHESF para tratar do tema do gerenciamento de riscos (DPR) mostra uma grande maturidade por parte da direção no que diz respeito ao tema. Este departamento trata da questão do risco de uma maneira universal, e não apenas de questões relacionadas à segurança da informação. Tal característica exige do DPR uma necessidade de associação com os mais diversos segmentos da empresa para o tratamento do tema. Num passado recente, o DPR liderou a formação de um comitê multidisciplinar formal, instituído pela diretoria da empresa para a avaliação dos riscos presentes em instalações das subestações da CHESF. Nesta ocasião, o comitê não foi permanente pois seu foco não era instituir uma política para toda a empresa, e sim, identificar e sanar vulnerabilidades ali existentes. Na elaboração do fórum para construção da Política de Segurança da Informação, fica nítida a necessidade de tratativa institucional similar.

6.0 CONCLUSÃO

A informação é um ativo crítico para as empresas do setor elétrico e requerem sérias preocupações no tocante à sua integridade, confidencialidade e disponibilidade. Neste cenário a elaboração de uma Política de Segurança da Informação se faz necessária. No entanto, esta empreitada em uma empresa do porte da CHESF, envolve muitas componentes e requer um grande esforço por parte da empresa. Algumas das dificuldades dizem respeito à ausência de uma metodologia bem definida para o desenvolvimento de uma solução eficaz,à extensão do tema dentro da empresa, que envolve praticamente todos os órgãos e exige comprometimento por parte da Diretoria, além das dificuldades técnicas.

O advento da SOX nas empresas do grupo Eletrobrás requer preocupações relacionadas ao controle da segurança da informação, no entanto, estas preocupações estão restritas aos domínios de segurança que envolvem os relatórios financeiros das empresas. A legislação permite às empresas uma certa flexibilidade na definição do escopo de TI a ser controlado e auditado. Na Eletrobrás, nenhuma aplicação operacional foi incluída no escopo de adequação à SOX. Na CHESF, foi possível perceber impactos indiretos positivos trazidos pela SOX.

A construção e implementação de uma Política Integrada de informação na CHESF, mais do que de iniciativas isoladas por especialistas das diversas áreas envolvidas, depende fortemente do respaldo da alta direção, da recriação de um comitê multidisciplinar formal, com representantes dos segmentos mais relevantes ao processo, como controle e automação, TI e Telecomunicações, do suporte de órgãos consultores externos, da análise de questões culturais e do *marketing* de segurança. Também são pontos chave para o sucesso de tal política a pesquisa e desenvolvimento na busca de soluções técnicas e padrões aplicáveis às empresas do setor, inclusive no tocante à questão da “segurança cibernética”.

REFERÊNCIAS BIBLIOGRÁFICAS

(1) IT CONTROL OBJECTIVES FOR SARBANES-OXLEY, IT Governance Institute, 2004, IL USA: *www.itgi.org* and *www.isaca.org.*

(2) Ericsson, Göran e Torkilseng, Åge, Management of Information Security for an Electric Power Utility—On Security Domains - IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 20, NO. 2, APRIL 2005.

(3) Ericsson, Göran e Torkilseng, Åge, Security for Information Systems and Intranets in Electric Power Systems – Technical Brochure – Cigré JWG D2/B3/C2-01, ver_2.2, June 27, 2006

(4) PROTECTION USING TELECOMMUNICATIONS, Cigré **J**oint Working Group 34/35.11 Final Report, December 2000.

(5) INTERNATIONAL STANDARD - ISO/IEC FDIS 27001:2005(E).

(6) PADRÃO INTERNACIONAL – ISO/IEC 17799:2000 (E).

DADOS BIOGRÁFICOS

Elton Bernardo Bandeira de Melo
Nascido no Caruaru, PE em 16 de junho de 1980.
Mestrando (previsto 2008) em Ciência da Computação na UFPE e Graduado (2002) em Engenharia Elétrica, modalidade Eletrônica na UFPE.
Empresa: CHESF – Companhia Hidro Elétrica do São Francisco, desde 2002.
Atua na Divisão de Engenharia de Manutenção e Reparo de Telecomunicações - DOMT
Membro do CIGRÉ-Brasil