SNPTEE
SEMINÁRIO NACIONAL
DE PRODUÇÃO E
TRANSMISSÃO DE
ENERGIA ELÉTRICA

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

GRUPO XVI

GRUPO DE ESTUDO DE SISTEMA DE INFORMAÇÃO E TELECOMUNICAÇÃO PARA SISTEMAS ELÉTRICOS – GTL

OS DESAFIOS NA IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA NAS REDES DE TELECOMUNICAÇÕES DA ELETRONORTE

Francisco Silva Dias **Nagib Bechara Pardauil *** **Rosemberg Lobato Silva**

CENTRAIS ELÉTRICAS DO NORTE DO BRASIL S.A. - ELETRONORTE

RESUMO

O crescimento e a convergências das redes de telecomunicações da Eletronorte, em um ambiente multi-fornecedor e multi-plataforma de gerência, suscitaram a necessidade de adoção de uma política de segurança voltada para as redes de telecomunicações. A implementação de uma política de segurança, envolve uma multiplicidade de aspectos técnicos, comerciais, jurídicos, culturais e comportamentais, políticos, etc. que, associados à definição dos ativos a serem protegidos e as responsabilidades por esta proteção, representam, em maio ou menor grau, desafios a serem superados na implementação de uma política de segurança. Saber o que defender e o motivo pelo qual deve-se defender constituem-se nos alicerces da política de segurança.

PALAVRAS-CHAVE

Segurança de redes; Operação de redes de Telecomunicações; Política de Segurança.

1.0 - INTRODUÇÃO

A expansão das redes de telecomunicações da Eletronorte, em um ambiente de multi-plataformas de gerenciamento e a convergência destas redes, resultou na necessidade de implementar uma política de segurança que, em diversos graus de complexidade, abrangem aspectos técnicos, comerciais, jurídicos, culturais, comportamentais, estratégicos e políticos e que se constituem em desafios a serem superados com vistas ao objetivo maior que é a segurança das redes de telecomunicações.

A implementação de uma política de segurança não se restringe apenas a resguardar pessoas, equipamentos e instalações e sim, especialmente, em resguardar o patrimônio intelectual e lógico dos sistemas e o próprio negócio da Empresa. Se por um lado, elaborar políticas de proteção ao patrimônio físico é algo palpável, proteger o patrimônio intelectual, o negócio e os ativos da empresa não é tão palpável assim, e apresenta desafio em sua implementação que se inicia pela definição dos ativos a serem protegidos, a que custos, a quem cabe protegê-los, como fazê-lo, etc..

O primeiro grande desafio a ser superado, corresponde à elaboração propriamente dita da política de segurança de redes de telecomunicações, que deve ser enxuta, baseada em princípios, separando-a dos detalhes de sua implementação, de forma a facilitar seu interesse e disseminação além de ser um convite à participação dos diversos atores envolvidos no processo.

(*) SCN Quadra 6, Conjunto. A, Bloco C, Sala 701 – CEP 70910-918 Brasília, DF – Brasil
Tel: (61) 3429.5355 – Fax: (61) 3328.6129 – Email: nagib@eln.gov.br

A definição dos ativos a serem protegidos e o estabelecimento de responsabilidades por esta proteção, são desafios importantes pois, saber o que se está protegendo e os motivos para tal, constituem-se na base para implementar a política de segurança.

Diversos são os desafios a serem suplantados para a implementação da política de segurança de redes de telecomunicações e, em análise mais ampla, de qualquer política de segurança mas, o principal desafio é o comprometimento das pessoas. É a partir da alteração dos padrões comportamentais das pessoas envolvidas no processo, da elaboração da política à sua aplicação, no que se refere à segurança. A superação deste desafio, ou pelo menos minorar os problemas daí advindos é uma tarefa contínua de "conquistar corações e mentes".

Este informe técnico encontra-se estruturado, apresentando as redes de telecomunicações da Eletronorte, a situação destas redes no que se refere à segurança, os desafios na implementação de uma política de segurança, aspectos da política de segurança e as perspectivas com a implantação desta política de segurança nas redes de telecomunicações da Eletronorte.

2.0 - REDES DE TELECOMUNICAÇÕES DA ELETRONORTE

Como saber o que se está defendendo constitui-se em um dos princípios da segurança de qualquer sistema, apresentamos a seguir as características básicas das principais redes de telecomunicações da Eletronorte, notadamente ópticas, em operação e que, por possuírem grande quantidade de estações, equipamentos e estações de trabalho e pela tendência de convergência do sistema de gerência para a rede corporativa da Empresa, necessita ser objeto de estudo mais detalhado no que se refere à segurança.

- Rede Tramo-Oeste : em operação desde 1998 e formada por sete estações e apresenta topologia em anel plano, ou seja, no mesmo cabo; utiliza equipamentos de tecnologia SDH, modelo SDM-1 e SDM-1C, de fabricação ECI e equipamentos de tecnologia PDH, modelo MP-2100 de fabricação RAD; estende-se ao longo de 622 km de cabos ópticos OPGW no estado do Pará. O sistema de gerência é composto por três plataformas distintas, quais sejam : "Radview 4.02", para gerenciamento de equipamentos de tecnologia PDH, desenvolvidos pela RAD; "eNM 7.5", para gerenciamento de equipamentos de tecnologia SDH, desenvolvido pela ECI e "Actionview 3.0", para supervisão de infra-estrutura, desenvolvido pela SPIN; a topologia da rede é cliente-servidor, com estações de gerência (SUN Ultra1), principal e reserva, localizadas em Brasília e estações remotas localizadas em Tucuruí e Altamira.

- Rede Norte-Sul : em operação desde 1999, é formada por sete estações da Eletronorte (há outras estações de Furnas), apresenta topologia radial e utiliza equipamentos de tecnologia SDH, modelo 1641 (óptico) e 9681 (rádio), de fabricação Alcatel e equipamentos de tecnologia PDH, modelos 1511 e 1515, também de fabricação Alcatel; o trecho da Eletronorte compreende aproximadamente 600 km de cabo OPGW e um enlace de 20 km de rádio digital; abrange localidades nos estados do Maranhão, Tocantins e Distrito Federal. O sistema de gerência é composto por uma plataforma única, com dois subsistemas de gerência : "Nectas 1320/1321NX", para gerência de equipamentos com tecnologia PDH; "1353EM/1354EM", para gerenciamento de equipamentos de tecnologia SDH, todos desenvolvidos pela Alcatel; a topologia é cliente-servidor, com estações de gerência (SUN Ultra 5), principal e reserva, instaladas em Brasília e estações remotas localizadas em Miracema.

- Rede Norte-Nordeste : em operação desde 2003 é formada por dezessete estações; apresenta topologia radial e utiliza equipamentos de tecnologia SDH, modelo XDM-1000, de fabricação ECI e equipamentos de tecnologia PDH, modelos MP-2100, MP-2104 e DXC-8R, de fabricação RAD; a rede compreende 1800 km de cabos ópticos OPGW, com estações localizadas nos estados do Pará e Maranhão. O sistema de gerência é composto de plataforma única, com dois subsistemas : "Radview 5.02", para gerenciamento de equipamentos de tecnologia PDH, desenvolvido pela RAD; "eNM-XDM", para gerenciamento de equipamentos de tecnologia SDH e "eNM 8.5", que agrega os outros dois sistemas, sendo estes últimos desenvolvidos pela ECI; a topologia da rede também é cliente-servidor, com estações de gerência (SUN Enterprise 420), principal e reserva, localizadas em Brasília, e estações remotas localizadas em São Luís, Imperatriz, Tucuruí e Belém;

- Rede Roraima : em operação desde 2001, é formada por cinco estações; apresenta topologia radial e utiliza equipamentos de tecnologia SONET, modelo FX155, de fabricação General Eletric; compreende 235 km de cabos ópticos OPGW, com estações localizadas no estado de Roraima e na Venezuela. O sistema de gerência é composto de plataforma única, "JNCI/JCI", para gerenciamento de equipamentos com tecnologia SONET, desenvolvido pela General Eletric; a topologia pe cliente-servidor, com estação de gerência (Windows NT), localizada em Brasília e estação remota localizada em Boa Vista;

- Rede Acre-Rondônia : em operação desde 2003, é formada por dezessete estações; apresenta topologia radial e utiliza equipamentos de tecnologia SDH, modelo 1650, de fabricação Alcatel e equipamentos de tecnologia PDH, modelo 1511, de fabricação Alcatel; a rede expande-se por 1400 km de cabos ópticos OPGW, com estações localizadas nos estados do Acre e Rondônia. o sistema de gerência é composto de

uma plataforma, “Nectas 1320-CT”, para gerenciamento de equipamentos de tecnologia PDH e SDH, desenvolvido pela Alcatel; a topologia é cliente-servidor, com estações de gerência (Windows 2000), principal e reserva, localizadas em Brasília e estações remotas localizadas em Porto Velho e Rio Branco;

- Rede Mato Grosso : em operação desde 2002, é formada por sete estações; apresenta topologia radial e utiliza equipamentos de tecnologia SDH, modelos MS1/4 e Fox 515T de fabricação, respectivamente, Marconi e ABB e equipamentos de tecnologia PDH, modelos XMP1 e Fox 515 de fabricação, respectivamente, Marconi e ABB; a rede expande-se ao longo de 785 km de cabos OPGW, com as estações localizadas no estado de Mato Grosso. O sistema de gerência é composto de uma plataforma, “SoA”, para gerenciamento de equipamentos de tecnologia PDH e SDH, desenvolvida pela Marconi e outra plataforma, “FoxMan”, também para gerenciamento de equipamentos de tecnologia PDH e SDH, desenvolvida pela ABB a topologia é cliente servidor, com estações de gerência (HP 3600), principal e reserva, localizadas em Brasília e estações remotas localizadas em Cuiabá e Rondonópolis;

- Rede Amapá : em operação desde 2001, é formada por oito estações, apresenta topologia radial e utiliza equipamentos de tecnologia SDH, modelo Fox 515, de fabricação ABB, compreendendo rede com 284 km de cabos ópticos OPGW, com estações localizadas no estado do Amapá. o sistema de gerência é composto de uma plataforma, “UNEM”, para gerenciamento de equipamentos de tecnologia PDH e SDH, desenvolvido pela ABB; a topologia é cliente servidor, com estações de gerência (Windows NT), principal e reserva, localizadas em Brasília e estações remotas localizadas em Santana;

- Rede WAN, constituída por 70 estações e quase cinco mil estações de trabalho, espalhadas por nove estados, possuindo equipamentos de diversos fabricantes, como Cisco, Allied, Alcatel, Huawey, Cyclades, dentre outros, utilizando redes de telecomunicações próprias e contratadas junto às operadoras de telecomunicações.O sistema de gerência é composto de uma plataforma, “CiscoWorks” e de uma plataforma “SNMPC-7”, para gerenciamento de equipamentos de rede (roteadores e switches), desenvolvidos pela Cisco e pela CRC; a topologia também é cliente servidor, com estações de gerência (Windows 2000), principal e reserva, localizadas em Brasília.

Além dos sistemas mencionados a Eletronorte, por meio de programa de pesquisa e desenvolvimento, implantou sistema denominado “gerência integrada” que, em verdade, coleta alarmes das estações de gerência proprietários para uma única plataforma (Windows 2000), facilitando a operação do centro de gerência, na identificação de anomalias e no acionamento das equipes de manutenção, pois há apenas uma plataforma a ser monitorada. Esta “gerência integrada”, não atua nos equipamentos, ou seja, depois de identificada a anomalia, as ações necessárias para sua solução são efetuadas diretamente na plataforma proprietária de determinado sistema de gerência.

3.0 - DESAFIOS NA IMPLEMENTAÇÃO DE POLÍTICA DE SEGURANÇA

Implementar política de segurança, e não importa a aplicação final, implica na superação de diversos desafios que se inicia e nunca termina nas pessoas envolvidas direta ou indiretamente no processo de segurança que, por ser um processo continuo não tem fim e sim aperfeiçoamento constante.

O primeiro desafio, se não o mais importante, é o convencimento das pessoas envolvidas com redes de telecomunicações, nas diversas escalas hierárquicas, da necessidade de implementar uma política de segurança e de sua importância estratégica para os negócios da Empresa, desmistificando de que a segurança não é apenas patrimonial e sim abrange aspectos pouco tangíveis, como a propriedade lógica e intelectual. Convencer pessoas a desenvolver e implementar uma política é tarefa complexa, pois envolve aspectos culturais destas pessoas e suas perspectivas com relação à credibilidade do trabalho a ser implementado, fruto de experiências negativas vivenciadas.

A seguir são apresentados alguns desafios que foram superados, ou ainda em de superação, verificados durante o processo de implementação da política de segurança de redes de telecomunicações e que não estão apresentados em ordem de prioridade ou importância :

- Definição do que venha a ser uma política de segurança : apesar de óbvio, estabelecer conceitualmente o que venha a ser uma política de segurança de redes de telecomunicações, e obter consenso entre todos os envolvidos sobre tal conceito é vital no estabelecimento de uma política. Muitos Homensxhora foram gastos, e ainda o serão, para que se buscasse consenso no que vem a ser a política de segurança;

- Evitar que a política tenha “proprietários” : a política não dever possuir “proprietários” e sim um grupo que se disponha a redigi-la e implementá-la, com a participação em maior ou menor grau das diversas pessoas envolvidas no processo de telecomunicações. Mesmo este grupo não pode ser considerado “proprietário”, quando muito apenas o coordenador da política. A superação deste desafio é algo estressante, pois atinge o ego das pessoas. Ações de convencimento de que todos poderão contribuir com o aprimoramento da política

nem às vezes ocasiona um efeito contrário, pessoas que poderiam contribuir não o fazem ou então contribuem negativamente com o processo;

- Multiplicidade de políticas : é uma conseqüência do acima mencionado, quando diversas áreas, às vezes subordinadas à mesma gerência ou diretoria, resolvem desenvolver suas próprias políticas de segurança de redes de telecomunicações, transformando a elaboração da política em uma competição de quem a implementa primeiro. Como envolve interesses diversos e conflitantes, a fronteira entre segurança da informação, muito em voga nas áreas de informática, e a segurança das redes de telecomunicações é tênue, a superação deste desafio merece boa dose de engenharia política;

- Definição dos ativos de telecomunicações a serem protegidos : saber o quê, o por quê e o como proteger, são itens primordiais na implementação da política de segurança. Na definição dos ativos é importante que se estabeleça uma classificação dos mesmos, que contemple o valor e a importância do ativo. Os ativos compreendem equipamentos, instalações, infra-estrutura incluindo cabeamento, documentação técnica, software de sistemas, estações de gerência Cada tipo de ativo apresenta uma característica diferente e diferentes formas de proteção. Esta classificação é importante, até para definir os custos e as prioridades com a implementação da proteção. Se o custo para proteger um determinado ativo, for superior ao valor e importância atribuídos ao ativo, então não valerá a pena protegê-lo;

- Redação e disseminação da política de segurança : redigir a política de segurança, de modo que o documento seja genérico, simples e direto, sem demasiados termos técnicos que dificulte sua leitura e sem perder o conteúdo e foco, é tarefa que prescinde de um bom redator e de bons revisores. A disseminação da política é um outro desafio superado pela divulgação por diversos meios, palestras e reuniões técnicas, etc., de tal forma a despertar o gosto pela implementação e pelo aprimoramento da política de segurança. Uma boa política que todos leiam, acessem e pratiquem, é melhor que uma excelente política que ninguém conhece;

- Atendimento às Leis : atenção especial deverá ser dada para que a política de segurança não viole a legislação em vigor no Brasil, em especial no que se refere à direitos previstos na Constituição Federal e legislação associada. A política não pode também, entrar em conflito com a política interna da Eletronorte;

- Contratos de confidencialidade : a implementação da política de segurança, pressupõe que todos os envolvidos, pessoal do quadro da Empresa e terceirizados, estejam cientes das implicações com a quebra das regras de segurança. No caso dos empregados da Eletronorte, os mesmos são regidos pelas normas internas da Empresa, sendo que a violação às mesmas poderá acarretar em sansões administrativas, culminadas com sansões jurídicas aplicáveis aos empregados de órgãos da administração pública. Mesmo neste caso, é importante que haja a celebração de contrato de confidencialidade, ou a implantação de código de ética, para solucionar questões com a violação à política de segurança. No caso de empregados terceirizados, os contratos são genéricos e não trazem explicitamente esta questão, devendo haver revisão nos contratos celebrados quer com empregados terceirizados ou com empresas terceirizadas de modo a resguardar a política de segurança. Empregados que exerçam atividades diretamente relacionadas à segurança das redes de telecomunicações, são o público preferencial na celebração deste modo de contrato. Este é um desafio ainda não superado, havendo poucas perspectivas que o seja em curto prazo, pelas implicações culturais, técnicas e jurídicas envolvidas;

- Fazer cumprir o estabelecido na política de segurança de redes de telecomunicações : é o desafio constante de cumprir e fazer cumprir as normas estabelecidas. Superar este desafio esbarra na resistência de alguns a seguirem as normas, de outros a descumpri-las sob o pretexto de estarem acima das normas, ou sob o pretexto de situações de emergência ou decisão superior. As diversas exceções para o não cumprimento da política de segurança, acabam por levá-la ao descrédito, frustração de quem participou do processo, e a conseqüente revogação da política por desuso;

- Criar uma cultura de segurança : desafio que se encontra associado à forma de disseminação da política de segurança e sua aplicação prática. Quando a política aproxima-se das atividades do dia-a-dia, e demonstra-se que e mesma não é um obstáculo e sim um ponto de apoio ao desenvolvimento das atividades, a criação desta cultura e o interesse pela mesma torna-se facilitado e que, se bem trabalhados, poderão contrapor-se ao possível não cumprimento da política de segurança;

- Capacitação técnica de pessoal sobre a política de segurança : desafio associado aos dois anteriores. Tanto a disseminação quanto a criação de uma cultura de segurança, dependem de programa estruturado de capacitação técnica sobre o assunto, devendo haver cursos específicos para específicas atividades relacionadas à segurança. Por exemplo, a equipe designada para operar a rede de telecomunicações, deverá ter capacitação diversa da equipe responsável pela auditoria de segurança desta rede. Como segurança é um processo contínuo de aprendizagem, o programa de capacitação técnica deverá prever treinamentos periódicos diferenciados, para todos os envolvidos com a rede de telecomunicações;

- Persistência da equipe responsável pela elaboração da política : como os desafios acima mencionados, nem sempre são superados na velocidade desejada, associados à desafios não tangíveis, como “vontade não expressa em haver uma política”, causam frustração e desmotivam a equipe, fatos estes que ocasionam atrasos em sua implementação total e uma elevada dose de persistência dos envolvidos diretamente no processo.

Alguns dos desafios para a implementação da política de segurança, são apresentados no item a seguir que apresenta alguns aspectos desta política.

4.0 - POLÍTICA DE SEGURANÇA PARA AS REDES DE TELECOMUNICAÇÕES

Foge ao escopo deste informe técnico o detalhamento da política de segurança para as redes de telecomunicações da Eletronorte, entretanto, algumas recomendações, consideradas relevantes, são apresentadas a seguir, antes porém, faz-se necessário definir alguns requisitos básicos à implementação da política de segurança, que se encontram baseados na tríade : integridade, disponibilidade e confiabilidade ou confidencialidade.

A integridade das redes corresponde à proteção contra alterações não autorizadas na configuração de equipamentos, sistemas, tráfego e conteúdo que trafega pela rede, de outro modo, garantir que a informação seja entregue ao destinatário sem modificação. A disponibilidade das redes corresponde à proteção contra interrupções, acidentais ou intencionais, dos dispositivos de telecomunicações desta rede, de outra forma, é garantir a continuidade dos serviços de telecomunicações e das informações que trafegam pela rede, corresponde também ao plano de contingência da rede de telecomunicações. A confiabilidade, confidencialidade ou privacidade, corresponde à proteção contra acesso não autorizado, tanto seja no sentido de alterar parâmetros de equipamentos e sistemas, tanto seja no sentido de violar, ou subtrair, as informações que trafegam pela rede de telecomunicações.

Algumas recomendações contidas na política de segurança de redes de telecomunicações da Eletronorte são :

- A política deve ser dinâmica e atualizada periodicamente, sendo ela mesma um processo contínuo de aprendizagem com as ameaças prováveis ou reais, com capacitação constante de toda a equipe de telecomunicações, em especial com a equipe responsável pelo suporte, manutenção e revisão da política de segurança;
- Estabelecimento de procedimentos de disseminação constante das práticas da política de segurança de redes de telecomunicações, para formar a cultura de segurança;
- Estabelecimento de prática de auditoria de segurança, realizando-se testes de conformidade entre o que se encontra estabelecido e a as atividades cotidianas relacionadas às redes de telecomunicações;
- Estabelecimento de mecanismos de verificação da segurança e os aspectos legais envolvidos, em especial com o não cumprimento da política de segurança
- Estabelecimento de prática de registrar e reportar à equipe de suporte de segurança quaisquer problemas verificados nos equipamentos os sistemas. Caberá à equipe de segurança verificar se o problema refere-se à violação ou não da política;
- Estabelecimento de padrão de sincronismo para toda a rede, de modo a permitir comparação de dados e confrontação de ações de violação ou de tentativas desta, facilitando a análise e a adoção de contra-medidas quando necessárias;
- Estabelecimento de plano de contingência, incluindo centros de contingência de operação, para interrupção parcial ou total em quaisquer pontos das redes de telecomunicações;
- A prestação de serviços para terceiros e a interligação destes às redes de telecomunicações, devem estar em conformidade com o que determina a política de segurança, evitando-se a instalação de quaisquer equipamentos sem a devida autorização, licença ou projeto técnico previamente aprovado;
- Acesso de terceiros, e também de empregados da Eletronorte, às instalações das redes de telecomunicações deverá estar em conformidade com a política de segurança de redes, evitando-se a presença de terceiros sem o acompanhamento de equipe da Eletronorte;
- Acessos para manutenção das redes de telecomunicações deverão estar previamente autorizados e devidamente acompanhados, especialmente se esta manutenção for autorizada, confrontando a manutenção realizada com a programada;
- Promover adequação, quando necessário, dos projetos de telecomunicações à política de segurança, incluindo a segurança patrimonial das instalações;
- Proibir alterações ou inclusões de “scripts” em estações de gerência, mesmo autorizados sob quaisquer pretextos, sem antes haver testes de performance e segurança que minimizem, ou eliminem, riscos à gerência das redes de telecomunicações;
- Evitar, sempre que possível, convergir para a mesma rede de telecomunicações a supervisão e gerenciamento destas redes e outras redes com acesso externo; caso não se possa evitar tal convergência, redobrar as recomendações explicitadas na política de segurança;
- Estabelecimento de política de contratação de pessoal, voltado para a segurança das redes de telecomunicações, em conformidade com as diretrizes da política de segurança adotando-se, sempre que

possível e em conformidade com a legislação vigente, acordos ou contratos de confidencialidade e as implicações advindas de sua violação;
- Estabelecimento de procedimentos que visem eliminar a utilização de senhas, para acesso aos sistemas de gerência, simples, repetitivas, de conhecimento comum, sem alterações periódicas e utilizadas pelos fabricantes dos sistemas, procurando-se utilizar processos de criptografia, sempre que necessário;
- Estabelecimento de procedimentos para o processo de geração, distribuição e armazenamento de chaves criptográficas incluindo criptografia para os “logs” de auditoria;
- Estabelecimento de procedimento para armazenamento de informações (banco de dados), incluindo: desenvolvimento; acesso; manutenção; descarte; espaço de armazenamento; duplicação; tempo de armazenamento; integridade, confiabilidade e disponibilidade das informações, etc.;
- Estabelecimento de procedimentos para preservação de banco de dados criação, manutenção, acesso e
- Promover, sempre que possível, a participação de outras áreas da Eletronorte, na condição de usuários das redes, na disseminação da política de segurança e no desenvolvimento de novas práticas de segurança das redes de telecomunicações.

Todas as recomendações acima mencionadas, ficarão restritas ao papel caso não haja engajamento e comprometimento de todos os atores envolvidos na política de segurança, para a sua implementação.

5.0 - CONCLUSÃO

A implementação da política de segurança das redes de telecomunicações da Eletronorte, ainda não superou todos os desafios encontrados. Alguns, inclusive, retornam com outra roupagem, requerendo novas técnicas de superação e que, de forma indireta, acaba por contribuir com o aperfeiçoamento da própria política.

Busca-se superar estes desafio através da disseminação dos conceitos do que vem a ser uma política de segurança para as redes de telecomunicações, ampliando o que alguns estudiosos em comportamento humano e suas relações com a administração, chamam de “massa crítica”, a partir da qual qualquer processo é deslanchado não havendo, ou sendo muito difícl, reversibilidade

Como a política de segurança para as redes de telecomunicações é um processo, a mesma deve estar em contínuo aperfeiçoamento que também é eivado de desafios, talvez até maiores que a implementação da política. O sucesso ou não da política de segurança, depende em sua excência da participação e da aceitação das pessoas às regras estabelecidas.

De nada adianta uma política bem estruturada se ninguém a cumpre. Este é um dos maiores desafios verificados : como convecer as pessoas a participarem, contibuirem com o aperfeiçoamento da política e manterem-se alertas às questões que envolvem a segurança, sem que a política caia em descrédito, antes mesmo de ser implantada, sem que seja considerada como mais um modismo e sim que seja encarada como uma necessidade, inclusive, à continuidade do negócio de telecomunicações da Eletronorte.

6.0 - REFERÊNCIAS BIBLIOGRÁFICAS

(1) ABNT NBR ISO/IEC 17799:2005 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação;

(2) Wadlow, T. A. – Segurança de Redes – Editora Campus, 2001;

(3) O funcionamento do Centro de Contingência para redes de telecomunicações em uma operação centralizada e descentralizada : Um estudo de caso da Operação das Redes de Telecomunicações da Eletronorte – Dias, F. S.; Pardauil, N. B.; IXI SNPTEE; Rio de Janeiro, 2007;