



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

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

**GRUPO - XV**

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

**VULNERABILIDADE DE DADOS: UMA VISÃO DE OPERAÇÃO DA TRANSMISSÃO DE ENERGIA ELÉTRICA**

**Mário Roberto Bastos (\*)  
CTEEP**

**RESUMO**

Uma vez que as empresas concessionárias de energia elétrica dependem de sistemas de informação para execução e continuidade de seu negócio, a Companhia de Transmissão de Energia Elétrica Paulista - CTEEP, como provedora de serviços críticos para a sociedade, se preocupa com o desenvolvimento de novos procedimentos e sistemas que propiciem melhorias em seus sistemas de Tecnologia de Informação e Comunicação, com especial ênfase em possíveis vulnerabilidades cibernéticas. Esta preocupação permeia as várias empresas do Grupo ISA de tal forma que, uma auditoria de Vulnerabilidade de Dados, está em andamento, de forma global e integrada, em todas as empresas do grupo nos seus países de origem, incluindo a própria CTEEP.

Esta auditoria busca avaliar a situação de segurança da informação, em cada uma das empresas; apontar soluções e ações a serem adotadas para mitigar quaisquer vulnerabilidades encontradas, assim como homogeneizar as soluções adotadas para todo o Grupo ISA. Neste trabalho serão apresentados: o contexto dos sistemas computacionais da CTEEP, sua relação com os sistemas das demais empresas do Grupo, o procedimento de teste de vulnerabilidade adotado pela auditoria, assim como o resultado da aplicação das recomendações propostas.

**PALAVRAS-CHAVE**

Segurança da Informação, Vulnerabilidade de Dados, Continuidade do Negócio, Sistemas de Supervisão e Controle

**1.0 - INTRODUÇÃO**

Atualmente as empresas dependem cada vez mais dos sistemas de informação e mesmo da Internet para fazerem seus negócios. Um incidente de segurança da informação que traga interrupções em suas atividades pode impactar negativamente as receitas da corporação, abalando a confiança de seus clientes, assim como o relacionamento com seus parceiros e fornecedores.

Fica, portanto, caracterizada uma relação direta entre incidentes de segurança, descontinuidades do negócio e prejuízos financeiros; fazendo com que a segurança da informação seja considerada como um dos pilares de suporte à estratégia de negócio da corporação. O seu gerenciamento passa a levar em consideração os elementos estratégicos da organização; evoluindo para uma extensão da prática de gestão de riscos (1).

Esta preocupação permeia as várias empresas do Grupo ISA de tal forma que, uma auditoria de Vulnerabilidade de Dados, está em andamento, de forma global e integrada, em todas as empresas do grupo nos seus países de origem (Figura 1), incluindo a própria CTEEP. Esta auditoria busca avaliar a situação de segurança da informação,

em cada uma das empresas; apontar soluções e ações a serem adotadas para mitigar quaisquer vulnerabilidades encontradas, assim como homogeneizar as soluções adotadas para todas as empresas (2).

O procedimento está estruturado em três fases macros, focadas na análise de riscos e levantamento das vulnerabilidades existentes nos sistemas atuais e na elaboração de recomendações.



Figura 1 – Contexto Geográfico

## 2.0 - METODOLOGIA

Na sua primeira fase, este procedimento envolveu uma análise de riscos, na qual se identificaram e relacionaram todos os recursos informáticos (estações de trabalho, roteadores, firewall, servidores, etc.) com impacto na continuidade do negócio da empresa. Uma vez identificadas, estas máquinas críticas são estressadas, através de ferramentas de software (PenTest) e conhecimento especialista do auditor, buscando-se encontrar pontos fracos de configuração de sistemas, vulnerabilidades de software, esquemas de senhas fracas, etc. que permitam explorar as vulnerabilidades identificadas, e que possam impactar em termos de quebra de sigilo, perda de integridade ou indisponibilidade dos dados e sistemas.

Uma vez que a CTEEP possui sistemas computacionais distintos em diversos níveis organizacionais, os testes necessitam ser efetuados de uma maneira hierárquica, em uma base multinível de modo a considerar todas as dependências entre estes vários sistemas. Em cada nível organizacional, as atividades de análise de riscos tiveram como resultado a identificação e quantificação do risco (vulnerabilidade), assim como a sugestão da ação a ser tomada de forma a mitigar as vulnerabilidades, eliminando-as ou tornando-as menos críticas (Figura 2).

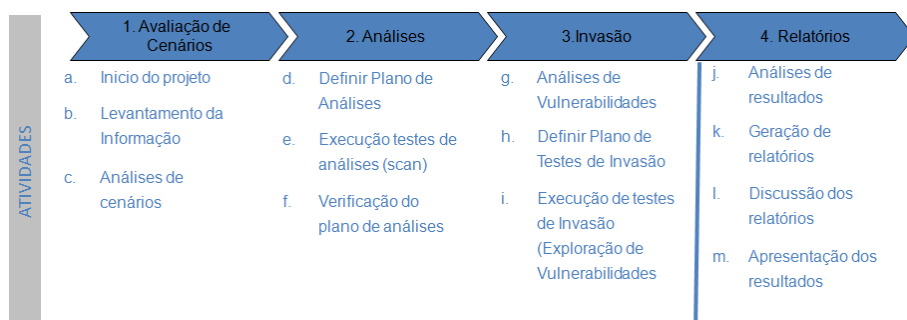


Figura 2 – Metodologia ©CTEEP

Na segunda fase do procedimento, a partir da adoção das recomendações, uma nova bateria de testes foi efetuada, verificando o atendimento às recomendações propostas e buscando obter o novo quadro atual dos sistemas de informação.

Na terceira fase, o processo será efetuado mais uma vez, no fim do qual será apresentado o resultado das implantações e atendimento às recomendações.

### 2.1 Objetivos

Os objetivos deste processo (2) buscam, através de um hacker ético externo e interno:

- A identificação de vulnerabilidades que possibilitem invasões externas (Internet) e internas (máquinas Pivô) às redes de dados das empresas do grupo;
- Analisar e informar o nível de segurança e gestão de segurança de toda a rede de dados, em todos os seus domínios de rede;
- Apresentar recomendações para mitigação das vulnerabilidades porventura encontradas.

A auditoria tem a duração programada de um ano, durante o qual serão efetuados três PenTest; dois dos quais já foram concluídos em 2010. O PenTest é constituído por um conjunto de métodos e ferramentas que permite verificar a robustez das soluções, adotadas visando o aspecto de segurança da informação.

### 2.2 Cenário dos Testes

Para a elaboração do cenário de testes foram consideradas as seguintes premissas:

- Cada uma das empresas forneceu a sua lista de equipamentos críticos;
- O auditor teve conhecimento dos endereços IPs dos equipamentos;
- O auditor não teve conhecimento da infraestrutura de rede do grupo.

Cada uma das empresas ficou responsável pelo envio de uma relação dos equipamentos, e respectivos endereços IPs, considerados críticos para o negócio da empresa, tanto corporativo, quanto operacional (Operação do Sistema Elétrico).

Máquinas adicionais (máquinas Pivô) foram inseridas na rede de dados de quatro empresas do grupo, sendo utilizadas como bases origem dos ataques internos à rede. A utilização destas máquinas Pivô se deu através de software remoto, com o propósito de uso mais eficiente dos canais de comunicação (Figura 3). O acesso à rede interna de cada empresa foi feito através de uma conexão VPN, cuja autorização e cancelamento de acesso foram acordados no cronograma inicial com cada uma das empresas.

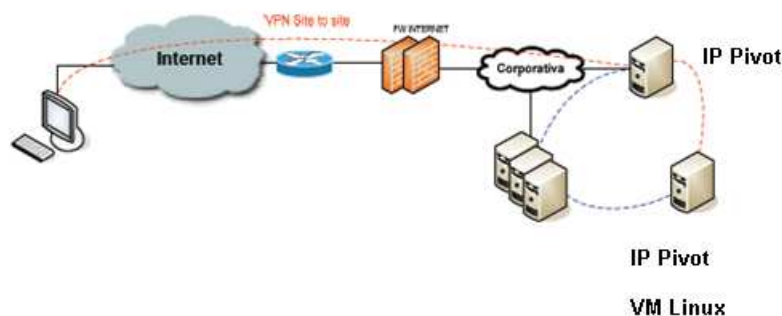


Figura 3 – Arquitetura Macro CTEEP

### 2.3 Rede de Operação – Sistema de Supervisão e Controle

Históricamente, a segurança dos equipamentos dos ambientes de Sistemas de Supervisão e Controle era baseada na obscuridade, uma vez que utilizavam protocolos proprietários e sistemas operacionais dedicados, além de ficarem restritos à sua própria rede. Esta situação alterou-se drasticamente devido a conversão dos Sistemas de Supervisão e Controle para o protocolo IP.

A disseminação do uso de protocolos, equipamentos e arquiteturas de redes padronizados e mundialmente difundidos, pode potencialmente apresentar as condições para a existência de vulnerabilidades, se não forem tomados certos cuidados.

Deve-se atentar para os seguintes tópicos:

- Excesso de confiança no perímetro
- Falta de monitoração
- Não entendimento dos riscos relacionados à mudanças
- Configurações não seguras
- Confiança cega no hardware e software proprietários

O Sistema de Supervisão e Controle da CTEEP (Rede de Operação) também foi objeto dos testes de vulnerabilidade, uma vez que está baseado em redes IP e existe um ponto de contato entre as redes Corporativa e de Operação. Existem aplicações que tornam disponíveis, no ambiente corporativo, o acesso à informações do Sistema de Transmissão.

Portanto, visando a manutenção dos altos índices de disponibilidade e integridade mesmo diante da possibilidade de ameaças, a Rede de Operação foi também considerada quanto aos testes de vulnerabilidades executados (Figura 4). Buscou-se verificar a existência de vulnerabilidades que pudessem permitir a invasão, a manipulação de informações e a indisponibilidade de serviços e/ou equipamentos.

<b>Técnicas de Scanning</b>	<b>Descrição</b>
TCP Connect	A identificação da porta é obtida mediante o estabelecimento de uma conexão TCP, buscando o estabelecimento do Three Hand-Shake.
SYN Scan	A identificação da porta é obtida mediante a resposta à uma tentativa de conexão na mesma. Com esta técnica se busca identificar as portas, sem deixar vestígios.
RST Scan	A identificação da porta é obtida mediante a resposta a uma tentativa de fim de conexão. Utiliza-se esta técnica para identificar sistemas de controle de acesso, como por exemplo, firewalls.

Figura 4 – Exemplos de Técnicas de Scanning

#### 2.4 Mitigação dos Riscos nos Testes de Invasão

Uma vez que os testes de invasão seriam efetuados em equipamentos em operação (em produção) houve a necessidade de se tomar certas medidas de forma a mitigar os riscos decorrentes das atividades do PenTest.

Desta forma, cada uma das empresas informou o horário, dentro do qual cada um dos equipamentos poderia ser objeto do PenTest.

Adicionalmente, a exploração de vulnerabilidades se realizou de forma a somente deixar-se uma evidência da mesma, sem gerar nenhuma indisponibilidade de serviços e/ou equipamentos.

Nenhuma vulnerabilidade, cuja exploração que já se sabia antecipadamente que poderia gerar riscos de indisponibilidades, foi efetivamente explorada. Sendo nestes casos, apenas registrada a sua existência

A empresa de Auditoria firmou um Acordo de Confidencialidade, de forma a garantir a não divulgação das informações utilizadas e/ou geradas.

E, considerando a possibilidade de que as atividades de exploração de vulnerabilidades, de alguma forma poderiam gerar indisponibilidades; em cada empresa foram monitoradas todas as fases do processo e caso necessário o auditor seria imediatamente informado de modo a interromper as atividades.

## 2.5 Relatórios de Vulnerabilidades

Em relação ao grau de riscos, a criticidade de uma vulnerabilidade em relação ao negócio está determinada pelo impacto na confidencialidade, integridade e disponibilidade da informação (2). Neste trabalho as vulnerabilidades foram classificadas como ALTA (vermelhas), MÉDIA (amarelas) e BAIXA (verdes), conforme ilustrado na Figura 5.

ALTA	MÉDIA	BAIXA
Permite autenticar e/ou obter informação de negócio disponível no equipamento	Permite obter usuários, informação parcial de negócio disponível no equipamento, ou acessar outros equipamentos	Permite obter informações de configuração para elaboração de ataques

Figura 5 – Classificação das Vulnerabilidades

Após as atividades do PenTest, foram gerados relatórios que relacionam as vulnerabilidades encontradas, sua criticidade, serviços e equipamentos afetados, ações recomendadas e referências para mais informações relativas à cada vulnerabilidade; podendo ser visualizado na Figura 6 um possível exemplo de vulnerabilidade.

Versão de OpenSSH exposta à múltiplas vulnerabilidades	
Através de análise da resposta do servidor, se identificou a versão de OpenSSH 4.3. Esta versão está exposta à múltiplas vulnerabilidades de diversas criticidades, que podem permitir a execução de código arbitrário, negação de serviços, entre outras.	
Porta(s) Associada(s):	TCP 22
Impacto:	Confidencialidade Disponibilidade
Criticidade:	Alta
Facilidade de exploração:	Média
Ação recomendada:	Atualizar para a versão mais recente do OpenSSH
Referências:	<p>Informações do fabricante:  <a href="http://www.openssh.com/txt/releas-5.3">http://www.openssh.com/txt/releas-5.3</a>  <a href="http://rhn.redhat.com/errata/THSA-2006-0697.html">http://rhn.redhat.com/errata/THSA-2006-0697.html</a></p> <p>Informação adicional:  <a href="http://www.securityfocus.com/bid/20214">http://www.securityfocus.com/bid/20214</a>            CVE-2006-5051 CVE-2008-4109 CVE-2008-1483</p>

Figura 6 – Exemplo de uma possível vulnerabilidade ALTA (2)

Na Figura 6, se apresenta a descrição da vulnerabilidade, quais as portas associadas à mesma, qual o impacto à segurança da informação, sua criticidade, facilidade de sua exploração, a ação recomendada para mitigar esta vulnerabilidade e referências relacionadas com a mesma (2).

Para cada uma das vulnerabilidades, cada empresa aplica as recomendações, verificando a compatibilidade das mesmas com as diversas aplicações residentes em cada equipamento.

Nos casos em que as recomendações não podem ser efetivadas, devido a incompatibilidades de pacotes de distribuição, versões de sistemas operacionais e/ou aplicações, estas exceções são registradas e informadas. Para cada uma delas, uma análise de risco é efetuada e alternativas são buscadas.

Quaisquer vulnerabilidades que não possam ser atendidas (por necessidade do uso pretendido) deverão ser relacionadas e justificadas. Posteriormente a Gerência deverá assinar termo responsabilizando-se pela situação, declarando-se ciente das implicações e riscos.

### 3.0 - CONCLUSÕES

No presente informe técnico apresentou-se e o processo de auditoria que busca avaliar a situação de segurança da informação, em cada uma das empresas interligadas; apontar soluções e ações a serem adotadas para mitigar quaisquer vulnerabilidades encontradas, assim como homogeneizar as soluções adotadas para todas as empresas do grupo.

Com a adoção das recomendações resultantes dos testes, o ambiente integrado de TI, contemplando todas as empresas em seus países de origem, torna-se homogêneo quanto às regras de segurança da informação e integridade funcional. De tal forma que os diversos processos organizacionais compartilhem a mesma solução.

Considerando, por exemplo, a inclusão ou mesmo substituição de um dos equipamentos, tem-se que garantir que este novo equipamento esteja aderente aos requisitos e correções/configurações (sistema operacional com patch atualizado, antivírus, serviços disponíveis, portas abertas, etc.) já adotadas e verificadas pelo último PenTest efetuado.

Observa-se, portanto, a necessidade de um procedimento formal a ser seguido, de modo a se manter as condições de segurança, assim como a monitoração contínua do ambiente computacional.

Com o avanço tecnológico, a definição das fronteiras de uma empresa torna-se uma tarefa cada vez mais difícil. As facilidades tecnológicas, por permitirem a conexão entre os diversos players e o compartilhamento de ativos e de informação, tornam a delimitação destas fronteiras empresariais cada vez mais complexa; resultando em uma maior gama de possíveis vulnerabilidades, ameaças e riscos. Conseqüentemente a gestão da segurança da informação torna-se também extremamente complexa.

Relembrando a relação entre vulnerabilidades e perdas financeiras, a segurança da informação passa a ser considerada como um investimento que auxilia a empresa a atingir seus objetivos de negócio.

### 4.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) ZAPATER,M.; SUZUKI, R. Segurança da Informação. Promon Business & Technology Review. 2005.
- (2) CTEEP. Auditoría a la Vulnerabilidad de la Red de Datos Grupo ISA. CTEEP, 2010.

### 5.0 - DADOS BIOGRÁFICOS



**Mário Roberto Bastos** é Engenheiro Eletricista, com ênfase em Eletrônica, pela Escola Federal de Engenharia de Itajubá (1985), especialista em Tecnologia de Informação (2002), Mestre em Engenharia (2006) e atualmente doutorando em Engenharia, todos pela escola Politécnica da USP. Possui 24 anos de experiência em sistemas de automação e controle e em engenharia de projetos. Trabalha, desde maio de 1994, na especificação técnica, desenvolvimento, implantação e manutenção dos Sistemas de Supervisão e Controle da CTEEP.