



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

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

**GRUPO -GTL**

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

**IMPLANTAÇÃO DA SEGURANÇA DA INFORMAÇÃO EM AMBIENTE DE TELECOMUNICAÇÕES**

**Armando Temporal (\*)  
CHESF – Companhia Hidro Elétrica do São Francisco**

**RESUMO**

Seguindo as diretrizes estabelecidas pelo Departamento de Segurança da Informação e Comunicações para a administração pública federal, a Chesf estabeleceu formalmente, no ano de 2009, a sua Política de Segurança da Informação, através de uma Instrução Normativa que estabelece explicitamente sua aplicabilidade ao segmento de Telecomunicações.

Esta questão foi abordada inicialmente pelo Departamento de Telecomunicações da Chesf com a realização do projeto "Análise de Riscos no Ambiente de Telecomunicações". Este Informe Técnico relata detalhes sobre a realização do projeto e como iniciar o desafio de implantar a segurança da informação em um ambiente de telecomunicações para uma empresa de energia.

**PALAVRAS-CHAVE**

Segurança da Informação, Análise de Riscos, Sistemas de Telecomunicações, Sistemas de Informação.

**1.0 - INTRODUÇÃO**

O tema Segurança da Informação é tratado como assunto de segurança nacional pelo Gabinete de Segurança Institucional da Presidência da República, através do seu Departamento de Segurança da Informação e Comunicações, que tem na sua missão "Planejar e coordenar a execução das atividades de segurança cibernética e de segurança da informação e comunicações na administração pública federal". O setor energético é um setor estratégico para o desenvolvimento de qualquer país, possuindo forte visibilidade política. Fazendo parte do setor elétrico e estando alinhada com as melhores práticas do mundo dos negócios, a Chesf estabeleceu formalmente em 2009, através de uma resolução normativa, sua Política de Segurança da Informação consonante com o seu planejamento estratégico. A política estabelece as diretrizes, normas e padrões que visam garantir um ambiente seguro e controlado para os ativos de informação a ela pertencentes. Tal política está amparada nas melhores práticas para a gestão da segurança da informação contidas na norma ABNT NBR ISO/IEC 27000 e explicitamente deve ser aplicável aos sistemas e equipamentos de automação e telecomunicações.

Foi também estabelecido um Comitê de Segurança da Informação e várias ações para a ampla divulgação interna da política foram e continuam sendo tomadas, de forma a torná-la acessível e disponível a todos. Não se pode negligenciar o fato de que grande parte da segurança da informação está sob responsabilidade do comportamento dos usuários, neste caso funcionários, estagiários e prestadores terceirizados que colaboram com o seu negócio. Tão importante quanto os sistemas de informação é que seus usuários estejam conscientes do seu papel e grau de influência no negócio da organização.

(\*) Rua Delmiro Gouveia, nº 333 – sala A-114 – Anexo II – CEP 50.761-901 Recife, PE, – Brasil  
Tel: (+55 81) 3229-4446 – Fax: (+55 81) 3229-4217 – Email: armandot@chesf.gov.br

Atualmente a segurança da informação tem papel chave na governança corporativa de uma organização. Cada vez mais os negócios são realizados de forma conectada e em tempo real, cujo ambiente computacional faz uso crescente de sistemas de informação. A segurança da informação procura manter o fluxo de informações seguro, obedecendo requisitos de disponibilidade, integridade e confidencialidade. Devem ser obedecidos, também, regulamentos e leis aplicáveis, além da capacidade de auditoria ao não repúdio, sendo o ator do acesso, uso, geração e alteração das informações registrado e unicamente identificado.

Observamos ainda uma convergência tecnológica que possibilita o uso de uma mesma tecnologia por segmentos distintos da mesma organização. Dados operacionais e administrativos compartilham a mesma infra-estrutura tecnológica. Observamos no setor elétrico segmentos organizacionais como os de automação, proteção, telecomunicações, tecnologia da informação e supervisão compartilhando uma mesma tecnologia, acarretando um aumento na vulnerabilidade quanto à segurança da informação.

Este Informe Técnico traz os resultados do primeiro projeto desenvolvido pelo Departamento de Telecomunicações da Chesf que atende à Política de Segurança da Informação corporativa, e busca trazer para o ambiente de telecomunicações da empresa a garantia de um ambiente seguro e controlado para os seus ativos de informação.

## 2.0 - ESCOPO DO PROJETO

Para atender às diretrizes estabelecidas pela Política de Segurança da Informação e buscar um ambiente seguro para os seus ativos de informações, o Departamento de Telecomunicações da Chesf aprovou a realização do projeto “Análise de Riscos no Ambiente de Telecomunicações”. De uma forma ampla, o objetivo do projeto é avaliar as vulnerabilidades existentes no segmento de telecomunicações que possam colocar em risco a segurança de suas informações para ser possível estabelecer um plano de ações direcionado, capaz de tratar as vulnerabilidades existentes. Ou seja, o principal objetivo é obter um diagnóstico do ambiente de telecomunicações.

O ciclo de vida para a gestão de vulnerabilidades (riscos) segue a mesma idéia do PDCA (*Plan, Do, Check, Act*). O planejamento corresponde ao inventário de recursos, a execução corresponde à análise dos riscos existentes, a verificação corresponde à avaliação dos resultados da análise de riscos e a ação corresponde ao tratamento das vulnerabilidades encontradas. O projeto realizado e aqui relatado consiste nas 3 primeiras fases deste ciclo. O tratamento das vulnerabilidades requer a realização de outros pequenos projetos, priorizados conforme critérios estabelecidos pela organização (recursos, impacto, prazo, etc.), que não fazem parte do escopo deste trabalho.

De uma forma mais detalhada, o projeto envolve a realização de um inventário dos recursos que suportam os processos de telecomunicações, a realização de um diagnóstico dos níveis de riscos associados a estes recursos, a elaboração de um plano de ações para o tratamento das vulnerabilidades encontradas, o estabelecimento de métricas e indicadores para o tratamento da segurança da informação e, ainda, a elaboração de instruções normativas para lidar com os processos críticos de telecomunicações.

O projeto contou também com uma ferramenta de apoio para a análise de riscos, o Risk Manager®. Foi estabelecida a premissa de que não haveria investimento em infra-estrutura tecnológica para uma ferramenta de apoio ao projeto, mas que seria utilizada a ferramenta já existente na Chesf, adquirida para o mesmo propósito pela Superintendência de Tecnologia da Informação. A ferramenta é utilizada no cadastro do inventário, mapeamento dos ativos com os sistemas que suportam os processos de negócios, os controles utilizados baseados nas recomendações de segurança da informação, estabelecimento das métricas para avaliação dos riscos e emissão dos relatórios resultantes das análises de riscos. Houve ainda com um treinamento para até 10 pessoas, incluindo membros de todas as divisões do departamento, que foram capacitados no processo de análise de riscos e no uso da ferramenta de apoio.

### 2.1 Inventário de Recursos

Para realização do inventário de recursos que suportam os processos de telecomunicações, os recursos foram separados em 4 tipos de ativos organizacionais, descritos a seguir:

#### a. Ativos tecnológicos;

Dentre os ativos tecnológicos escolhidos, buscou-se abranger todo o sistema de telecomunicações fazendo uma amostragem que representasse todo o sistema. Não se fez necessário, por exemplo, cadastrar todos os roteadores e switches da rede. Foi feita uma amostragem de um grupo representativo de tal forma que os demais ativos do mesmo tipo são repetições daqueles escolhidos. Obviamente, quando a análise for realizada e forem apresentados os pontos de vulnerabilidades, o plano de ação deverá considerar que a aplicação das correções será realizada em todos os ativos, não apenas no grupo que foi analisado. O importante é tomar um grupo que represente de fato todo o escopo do sistema (e.g. incluir roteadores de borda, de núcleo, etc.). Este grupo de ativos compreende

roteadores, switches, complexos de rede (LAN/WAN), servidores de gerência com diversas finalidades e estações de trabalho dos colaboradores.

Ainda com respeito aos ativos tecnológicos, foi dado tratamento diferenciado a um subconjunto chamado de ativos específicos de telecomunicações. A razão para este tratamento diferenciado será explicada posteriormente. Este subconjunto contempla as seguintes especialidades: teleproteção (modem e equipamento de telesupervisão), transmissão (rádio, multiplexador e concentrador), vídeo (MCU e codec) e comutação (central telefônica, gravador digital de voz e tarifador). Buscou-se sempre avaliar equipamentos de diferentes fabricantes e, quando possível, diferentes tecnologias.

b. Ambientes físicos;

Para os ambientes físicos avaliados foram escolhidos locais considerados estratégicos para manutenção do sistema de telecomunicações, utilizando também uma amostragem representativa dos ambientes existentes. Foram escolhidos o CPD que hospeda todos os servidores de gerência, duas salas de telecomunicações localizadas em subestações cuja complexidade é bastante significativa, e o laboratório de ensaios que hospeda o modelo reduzido de telecomunicações. Os ambientes escolhidos são avaliados juntamente com o seu entorno, como o prédio que o acomoda e sua acessibilidade.

c. Recursos Humanos;

Foram selecionados vários colaboradores para avaliação, considerando inclusive a participação de terceirizados neste processo. A amostra contou com funcionários de todas as divisões, em diversos papéis e responsabilidades. Foram escolhidos gestores em vários níveis, engenheiros, técnicos e assistentes administrativos, abrangendo também os serviços regionais de telecomunicações.

d. Processos Organizacionais;

A escolha dos processos organizacionais para avaliação das vulnerabilidades foi uma decisão trabalhosa. Nos demais ativos é mais fácil escolher uma amostra que represente significativamente o conjunto total dentro do sistema de telecomunicações. No caso dos processos organizacionais a escolha levou em consideração processos que reflitam as tarefas e rotinas do trabalho diário, que sejam bastante críticos, e que mesmo não sendo realizados diariamente tenham um significado importante para a continuidade do negócio de telecomunicações dentro da Chesf. Foram escolhidos os processos que tratam das ordens de serviço, das intervenções e acessos às instalações, da gestão dos ativos de telecomunicações, da gestão dos normativos de telecomunicações, e dos procedimentos de backup dos ativos tecnológicos (servidores de gerenciamento ou configuração de equipamentos).

## 2.2 Elaboração do Mapa de Governança

De posse dos ativos (recursos) a serem considerados na avaliação de vulnerabilidades, o passo seguinte consistiu na elaboração do mapa de governança do segmento de telecomunicações. O objetivo final da montagem do mapa de governança é mapear como os ativos inventariados influenciam os processos de negócio do segmento em estudo. Dessa forma é possível identificar como a vulnerabilidade de um ativo irá deixar indiretamente vulnerável um processo de negócio da organização – leia-se como organização o segmento de telecomunicações. Dado o elevado número de ativos inventariado não é possível exibir o mapa geral de governança no espaço de uma folha de papel, mas para o entendimento de como este processo de mapeamento é realizado, um mapa de governança simplificado é apresentado como ajuda no entendimento – ver Figura 1.

Na camada superior estão os processos de negócios (ou componentes de negócio) do sistema organizacional, que no nosso caso é o Departamento de Telecomunicações da Chesf. Estes processos de negócio são suportados por sistemas ou serviços, que podem ser por exemplo um sistema de transmissão ou comutação de dados, um serviço regional de telecomunicações, um ERP ou qualquer sistema/serviço que faz com que o processo de negócio possa existir ou dê apoio direto à sua funcionalidade. Estes sistemas encontram-se numa camada intermediária e são diretamente servidos ou apoiados pelos ativos organizacionais inventariados. Pode-se entender, por exemplo, que um processo de negócio é suportado por um sistema de informação, e este por sua vez está hospedado num servidor que tem um administrador na pessoa de um funcionário, e está fisicamente situado numa sala apropriada para este fim. Neste caso, mais de um ativo suporta o serviço.

Assim é feito o mapeamento de todos os ativos que apoiam os processos de negócio. É possível imaginar que uma vulnerabilidade existente em algum dos ativos vai implicar num reflexo de vulnerabilidade no processo de negócio que ele apoia. Extrapolando-se essa idéia para uma grande quantidade de ativos que suporta um mesmo processo de negócio percebemos que no sentido da camada inferior (ativos) para a camada superior (processos de negócio), quanto mais ativos vulneráveis existirem aumenta-se o risco do negócio em questão. No sentido inverso, um processo de negócio crítico aumenta a criticidade dos ativos que o suportam, obrigando a existência de controles que aumentem sua segurança.

Lembrando que foram inventariados 4 tipos de ativos (tecnologia, recursos humanos, ambiente físico e processos

organizacionais). Para cada tipo foi tomada uma quantidade significativa de ativos e percebe-se a dimensão e complexidade deste mapa de governança e a razão de não ser possível apresentá-lo aqui. A construção do mapa de governança é uma atividade realizada com a ajuda de vários profissionais das mais diversas especialidades do segmento de telecomunicações, que conhecem profundamente o negócio do segmento organizacional ao qual pertencem, possuem uma visão do todo, e são capazes de apoiar no mapeamento entre processos de negócio, sistemas e ativos. Trata-se de uma tarefa complexa, que consome bastante tempo e conta com o apoio dos colaboradores. É natural que uma revisão neste mapa de governança sempre vai apontar pequenas mudanças ou ajustes de melhoria, assim como uma revisão neste Informe Técnico, mas cujas alterações (que devem ser pequenas) não comprometem o resultado final do trabalho realizado.

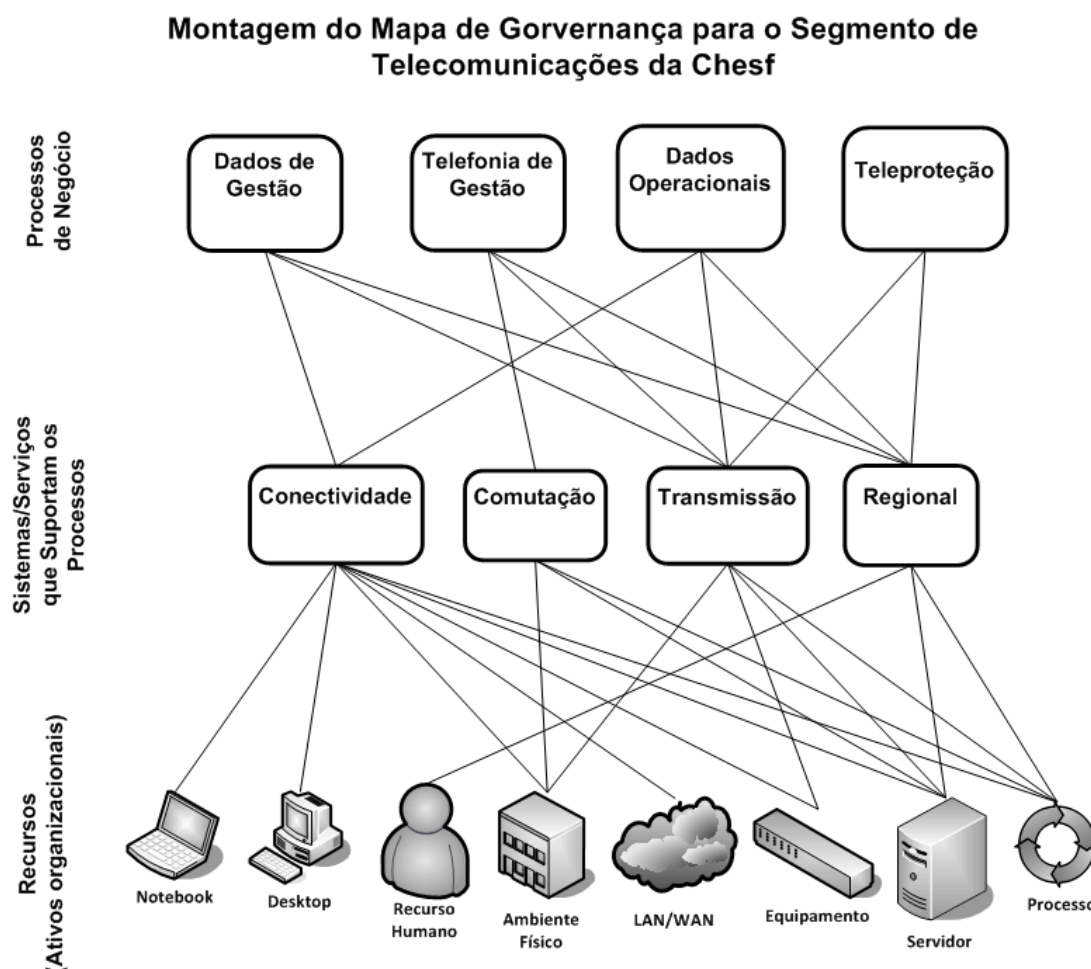


FIGURA 1 – Exemplo Simplificado de um Mapa de Governança

### 2.3 Análise de Vulnerabilidades

A análise de vulnerabilidades, ou análise de riscos, é realizada em cada um dos ativos inventariados através da verificação de controles aplicáveis. Existem as recomendações, que são em sua maior parte definidas nas normas ISO, por exemplo as normas da família 27000, e existem as boas práticas entendidas assim pela comunidade internacional que estuda o tema, ou mesmo por fabricantes de equipamentos e aplicativos que divulgam à comunidade suas recomendações para manter seus ativos o mais afastado possível de vulnerabilidades. Essas fontes distintas de recomendações geram o que são conhecidas por Bases de Conhecimentos (KB – *Knowledge Base*). O conjunto de KB aplicáveis a um mesmo ativo dá origem a um questionário de controles. Dessa forma, um questionário de controles pode estar baseado em mais de uma KB, mas normalmente um controle individual está baseado em uma única KB. Ao controle é associado um valor chamado PSR<sup>®</sup> que representa o quão crítico é aquele controle para o ativo em análise. Aproveitando as definições da NBR ISO/IEC 17799 controles são políticas, práticas, procedimentos, estruturas organizacionais, funções de software e dispositivos de hardware voltados à segurança que visam reduzir ou eliminar vulnerabilidades, inibir a ação de agentes e ameaças, ou ainda minimizar impactos causados por incidentes. Essencialmente são implementações que foram consideradas necessárias para redução do risco ou minimização dos seus impactos.

Um risco pode ser entendido como uma incerteza. Se a incerteza é conhecida temos condições de traçar um plano capaz de mitigá-la ou eliminá-la. O maior problema é não conhecer que um risco existe e assim não ter planejada nenhuma ação para evitar que o mesmo se torne um problema ou mesmo que o seu impacto, caso ocorra, seja reduzido. Uma definição de risco encontrada na norma ISO/IEC Guide 73 diz que o risco é "a combinação da probabilidade de um evento e sua consequência". Ou seja, existe um evento incerto e tal incerteza se dá pela probabilidade associada ao evento. Tal evento, caso ocorra, tem um impacto revelado pela consequência. A nossa avaliação de riscos considerou a combinação dessa probabilidade com o impacto gerado e ainda levou em consideração a importância daquele ativo para o negócio da empresa, considerando os processos de negócio que ele apoia. Esta combinação representa o grau de risco associado à ausência de um controle e o chamamos de PSR<sup>®</sup>, conforme a equação:

$$\text{Risco (PSR}^{\text{®}}\text{)} = \text{Probabilidade} \times \text{Severidade} \times \text{Relevância}$$

- a. Probabilidade: probabilidade da vulnerabilidade ser explorada pelas ameaças por falta de controles;
- b. Severidade: consequência na segurança da informação caso as ameaças explorem a vulnerabilidade;
- c. Relevância: importância do ativo para o negócio, dados os componentes de negócio que ele apoia.

O formato utilizado para estabelecer um critério numérico para o cálculo de um PSR<sup>®</sup> é associar os níveis de muito baixo a muito alto numa escala de 1 a 5 para cada uma das variáveis P (probabilidade), S (severidade) e R (relevância). Neste caso os valores possíveis de PSR<sup>®</sup> para um controle qualquer variam de 1 a 125, não sendo possíveis quaisquer valores, mas apenas os resultados da combinação das 3 variáveis que assumem valores de 1 a 5. Quanto maior o valor do PSR<sup>®</sup> maior o risco associado à não implementação daquele respectivo controle.

No questionário de controles, um controle pode ter sua situação descrita como:

- a. Implementado
- b. Não implementado
- c. Não aplicável
- d. Não respondido

Quando um controle aplicável não é implementado, seu valor de PSR<sup>®</sup> é adicionado ao valor de PSR Total e essa quantidade será utilizada posteriormente como indicador do nível de risco.

#### 2.4 Ativos Específicos de Telecomunicações

Foi comentado anteriormente sobre o tratamento especial dado a um subconjunto de ativos tecnológicos, os ativos específicos de telecomunicações (ativos de teleproteção, transmissão, vídeo e comutação). Para estes ativos não existia ainda uma KB (específica) que pudesse ser utilizada pelos controles para avaliação das vulnerabilidades. A solução encontrada foi desenvolver uma KB específica para este subconjunto de ativos tecnológicos com a finalidade de gerar o questionário de controles. Levou-se em consideração cada uma das especialidades com suas características específicas de probabilidade e severidade, não confundindo as especialidades entre si. Cada especialidade teve sua KB desenvolvida, que na essência possui os mesmos controles, entretanto com probabilidade e severidade específicas. No caso da relevância, a mesma é atribuída na avaliação de riscos para cada ativo, conforme seu apoio aos processos de negócio.

Vale ressaltar que na construção de KB específicas leva-se em consideração não apenas o equipamento em si, mas também sua localização física, ambiente de instalação, condições de alimentação e os colaboradores que tenham acesso físico e lógico ao equipamento. Questões contratuais, procedimentos operacionais, aspectos de gerência remota e manutenção são também considerados. A construção de uma KB específica conta com o conhecimento e a ajuda dos especialistas responsáveis por aquele ativo, capaz de fornecer informações precisas quanto a suas características técnicas e relevância para o sistema de telecomunicações. Foram criados mais de 100 controles para cada uma destas KB específicas.

#### 2.5 Indicadores de Segurança da Informação

Para avaliação dos resultados da análise de riscos foram utilizados os seguintes indicadores:

- a. Indicador de Risco Absoluto (PSR Total): é a soma direta de todos os valores de PSR<sup>®</sup> dos controles não implementados;
- b. Indicador de Conformidade: é um indicador percentual de avaliação quantitativa que divide o total de controles implementados pelo total de controles aplicáveis;
- c. Indicador de Segurança: é um indicador percentual de avaliação qualitativa que divide o total de riscos dos controles implementados (PSR Evitado) pelo total de riscos dos controles aplicáveis (PSR Total)

Dos indicadores utilizados, os dois últimos são os mais significativos, uma vez que revelam diretamente uma aderência aos controles (indicador de conformidade) ou uma aderência aos controles ponderada pela sua

probabilidade, severidade e relevância (indicador de segurança). Vários relatórios podem ser obtidos, fazendo-se uma extratificação dos ativos por tipo, estabelecendo-se critérios para os níveis de riscos e conformidade, ou por base de conhecimento (KB), por processo de negócio, ou mesmo por responsável. Apresentaremos os resultados mais significativos e representativos, afinal uma extratificação serve para definir quais as linhas de atuação dos projetos que serão adotados para atacar as vulnerabilidades.

## 2.6 Resultados da Análise

A ferramenta de apoio fornece vários relatórios e com níveis de detalhamento distintos. Cada relatório tem uma finalidade específica e alguns devem ser tratados com confidencialidade, uma vez que expõe nomes de pessoas e quais os níveis de vulnerabilidades a ela associados. É bem verdade que muito da vulnerabilidade encontrada num recurso humano investigado está revelada pela sua honestidade e transparência na resposta ao questionário de avaliação do seu comportamento, seja como gestor ou usuário. Da mesma forma, a avaliação de alguns ativos tecnológicos depende muito da fidelidade de resposta de algumas perguntas feitas aos seus responsáveis ou especialistas. Para se ter uma idéia da dimensão dos controles investigados, foram investigados 17.723 controles dos quais 16.676 foram considerados controles aplicáveis.

Os principais resultados obtidos na análise de riscos são listados a seguir:

- a. O indicador de conformidade encontrado (controles implementados) foi de 43,75%;
- b. O indicador de segurança resultante (riscos evitados) foi de 45,51%;
- c. Quando são considerados todos os ativos, das 10 maiores vulnerabilidades 7 são de recursos humanos e 3 são de processos organizacionais;
- d. Se forem considerados apenas ativos de tecnologia, os indicadores de conformidade e segurança serão iguais a 66,68% e 73,37%, respectivamente;
- e. Se forem considerados somente recursos humanos, os indicadores de conformidade e segurança serão iguais a 41,35% e 39,15%, respectivamente;
- f. Se forem excluídos os recursos humanos da análise, os indicadores de conformidade e segurança serão iguais a 43,87% e 45,89%, respectivamente. Neste caso, dos 10 maiores riscos 3 são de processos e os demais são de ativos tecnológicos.

## 2.7 Instruções Normativas

O projeto ainda contemplou a escrita de Instruções Normativas, baseadas nas necessidades identificadas com os resultados obtidos da análise de vulnerabilidades. O processo de escrita foi aberto para participação e contribuição de todas as divisões do departamento. O objetivo das instruções normativas é dar as diretrizes internas a serem seguidas, com base nas normas e recomendações existentes e nas vulnerabilidades identificadas. Estas instruções escritas refletem a necessidade de controles para manutenção de um ambiente de telecomunicações seguro e ao final do projeto necessitam de aprovação superior e posterior publicação. Foram definidas e formuladas 12 instruções que abordam os assuntos listados a seguir:

- a. Controle de Acesso;
- b. Cópias de Segurança;
- c. Gestão de Ativos e Classificação da Informação;
- d. Gestão da Capacidade;
- e. Gestão da Conformidade da Segurança da Informação;
- f. Gestão da Continuidade do Negócio;
- g. Segurança Física;
- h. Gestão de Incidentes de Segurança da Informação;
- i. Gestão de Mudanças;
- j. Segurança em Recursos Humanos;
- k. Gestão de Riscos;
- l. Gestão de Segurança da Operação dos Sistemas;

## 3.0 - CONCLUSÃO

O desafio proposto por este trabalho contou com a ajuda e disponibilidade de várias pessoas integrantes do Departamento de Telecomunicações da Chesf, cujo apoio para a conclusão do escopo de todas as atividades dentro do prazo estabelecido foi fundamental. O projeto teve duração total de 5 meses, com as atividades de execução concentradas num período de 4 meses. A realização de um inventário dos recursos (ativos) pertencentes ao departamento e o posterior exercício para elaboração de um mapa de governança amadurecem bastante a visão da dimensão do negócio de telecomunicações dentro da empresa e serve de oportunidade para que sejam revistas todas as atividades, prioridades e processos de negócio. Pode-se dizer que houve um ganho de amadurecimento quanto ao negócio desempenhado e sua importância no contexto da empresa.

Observando-se os resultados da análise das vulnerabilidades percebe-se que a maior parte delas está nas mãos das pessoas e processos operacionais. Os colaboradores são os grandes responsáveis pela segurança do ativo de informação no ambiente de telecomunicações. Assim também são os processos operacionais executados pelas pessoas, que desempenham papel fundamental no apoio aos sistemas e no suporte aos componentes de negócio (processos de negócio). Observa-se também que mesmo considerando apenas os ativos tecnológicos ainda existe bastante espaço para aperfeiçoamento da plataforma tecnológica no tocante à segurança da informação.

Vale ressaltar que os consultores externos que apoiaram o projeto revelaram que para uma primeira abordagem de análise de riscos os valores estão dentro do esperado e encontrado usualmente nas empresas que realizam um primeiro diagnóstico. O mais importante neste momento é possuir um diagnóstico do ambiente de telecomunicações e ser possível direcionar esforços para atuar na melhoria dos indicadores de conformidade e riscos. As ações a serem tomadas devem considerar seus impactos, custos, tempo, viabilidade de implementação, disponibilidade de recursos, cultura organizacional, dentre outros. Uma vulnerabilidade mapeada pode ser considerada aceita e apenas monitorada periodicamente, mas sua identificação já traz ganhos para o sistema organizacional. Como resultado significativo obtido com a realização do projeto pode-se também citar a elaboração de um conjunto de instruções normativas embasadas nas recomendações e boas práticas internacionais, alinhadas com os resultados da análise realizada e com a realidade do segmento de telecomunicações da Chesf. Estas normas dão as diretrizes que devem ser tomadas.

Os resultados deste trabalho abrem espaço para a realização de vários outros pequenos projetos que tratem das vulnerabilidades identificadas e os desafios continuam para que um melhor desempenho possa ser obtido numa análise de vulnerabilidades futura. Procedimentos operacionais, baseados nas instruções normativas foram também discutidos mas precisam ser revalidados, pois trata-se de tarefa posterior ao projeto e de escopo operacional e interno.

#### 4.0 - REFERÊNCIAS BIBLIOGRÁFICAS

- (1) Família ISO/IEC 27000, International Organization for Standardization
- (2) ABNT NBR ISO/IEC 17799
- (3) ISO/IEC Guide 73 – Risk Management Vocabulary
- (4) <http://www.gsi.gov.br>, março de 2011
- (5) <http://dsic.planalto.gov.br>, março de 2011
- (6) Documentação do projeto “Análise de Riscos em Ambiente de Telecomunicações”, Chesf 2010/2011
- (7) Edison Fontes, Segurança da Informação – o usuário faz a diferença, Editora Saraiva 2006
- (8) Anderson Ramos et al, Security Officer 1 – Guia Oficial para Formação de Gestores em Segurança da Informação, Editora Zouk, 2008

#### 5.0 - DADOS BIOGRÁFICOS

##### **Armando Temporal Neto**

- Nascido em Recife-PE em 14 de agosto de 1975;
- Graduado em Engenharia Elétrica/Eletrônica pela Universidade Federal de Pernambuco – UFPE em 1998;
- Mestre em Engenharia Elétrica na área de Sistemas de Comunicações pela Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio em 2000;
- Certificado PMP (Project Management Professional) pelo PMI (Project Management Institute) desde 2007;
- Professor em diversas instituições de cursos de pós-graduação em gerenciamento de projetos;
- Instrutor do PMI - capítulo Pernambuco para cursos de gerenciamento de projetos;
- Engenheiro do Departamento de Telecomunicações da Chesf na Divisão de Manutenção – DOMT.