

Segurança e Auditoria da empresa Centrais Elétricas Light – CEL

Flávio Ferreira dos santos
José Francisco
Virgínia de Sousa
Yuri Aguiar

Resumo

A Segurança da Informação nas organizações tem sido o principal desafio a ser alcançado. As corporações estão cada vez mais dependentes dos Sistemas de Informação e por isso a missão de se formar um ambiente computacional seguro tem se tornado tão importante. Existe um grande potencial de perdas na ocorrência de desastres, falhas na infra-estrutura e paradas dos sistemas. No caso de uma empresa distribuidora de Energia Elétrica, qualquer mínima falha poderá comprometer o abastecimento de energia para milhares de pessoas e empresas afetando diretamente a economia , podendo causar perdas irreparáveis e irreversíveis e até mesmo perdas financeiras. A Segurança de um módulo de manutenção e administração de equipamentos pode ser o tanto mais importante quanto maior for a área de atuação da empresa em questão. Por isso a necessidade de planejar de forma correta o plano de segurança de uma organização com este perfil, levando em consideração a Criticidade, as medidas preventivas e capacidade de recuperação diante de algum dano.

Palavras-chave

Segurança da Informação, Plano de Contingência, Sistemas de Informação, Energia Elétrica, Objetivos Organizacionais, Informação, Criticidade, Segurança, Tecnologia da Informação (T.I.) , Plano de Segurança, Sistemas de Informação (S. I.).

1. Introdução

A política de segurança da informação deve basear-se no código de prática para gestão da segurança da informação a ISO/IEC 17799 de Agosto de 2001. Esta norma que é caracterizada pela preservação de Confidencialidade, Integridade, Disponibilidade das informações, é essencial para a imagem da organização em geral. Esta norma irá fornecer as orientações necessárias para a montagem do plano de segurança da informação.

Cada vez mais as empresas são colocadas à prova de diversos tipos de ameaças e o controle da segurança da informação bem como seus planos de contingência são infinitamente mais baratos e eficientes no combate destes imprevistos do que a busca de recuperação de perdas.

A elaboração de um Plano de Contingência é uma tarefa importantíssima que normalmente envolve diversos setores da organização e o mesmo abrange vários aspectos:

- Análise de riscos;
- Análise de impactos;
- Estratégicas de recuperação;
- Treinamento;
- Manutenção e revalidação;
- Documentação segura dos processos definidos;

É necessário que as empresas identifiquem seus requisitos de segurança pois a partir deles podem ser planejados os riscos de segurança, as ameaças, as vulnerabilidades e a probabilidade de ocorrência de falhas. Com a avaliação destes fatores definidos o próximo passo é direcionar e determinar as ações gerenciais necessárias e adequadas para controle de riscos envolvidos.

2.1 Integração

A integração do Processo PM é extremamente forte dentre os demais módulos de Materiais e Financeiros, na medida em que a padronização dos procedimentos de linguagem entre as diversas áreas da empresa exercem um fator bastante importante. Com a otimização da utilização de mão-de-obra o sistema pode mensurar os custos de manutenção; pode prever os custos a serem realizados com um todo, e também, pode guardar este histórico financeiro.

Na avaliação de disponibilidade de materiais é ressaltada uma lista de sobressalentes associada a cada equipamento e a partir da Ordem de Manutenção foi viável uma criação de planos de manutenção plurianual. Desta forma o sistema consegue controlar um histórico técnico, acompanhando estatísticas e análise de desempenho de cada equipamento.

Os ganhos com a Ferramenta R/3 foi de fundamental importância pois o processamento passou a ser em tempo Real. Um exemplo foi a associação de documentos técnicos (Módulo DMS – Gerenciador de Documentos, previsto implantação no 2º semestre de 2001) ao equipamento ou local de instalação provendo uma maior flexibilidade de relatórios.

2.2 Análise da Criticidade

Para decidir o nível de investimento em proteção, é preciso também, analisar o grau de criticidade de cada sistema e o impacto operacional de sua parada em toda corporação.

O módulo PM está caracterizado na matriz de criticidade, como um módulo que tem alta necessidade de medidas preventivas e também alta necessidade de capacidade de recuperação.

De acordo com a ABNT-ISO.IEC 17799:2001, Item 3.1.2 – Análise Crítica e Avaliação, foi definida a Estrutura Funcional do Grupo de Trabalho de Gestão Empresarial, o qual tem como gestor o Comitê Técnico de Gestão.

Administração de Objetos Técnicos (Dados Mestres – Local de Instalação, Cadastro de equipamentos, Lista Técnica Sobressalentes); Planejamento de Manutenção e Serviços (Execução de Serviços, controle e estatística de serviços realizados; Planejamento de Disponibilidade de mão-de-obra das equipes de manutenção e operação; Manutenção Preditiva (é a manutenção baseada na condição do equipamento). A disponibilidade deve ser de aproximadamente 95%, considerando 24 horas por 7 dias na semana.

2.3 Políticas de Segurança e Contingência de Rede

A CELTI – Superintendência de Tecnologia da Informação é a área responsável pela Rede NetCEL com mais de 2.500 usuários trafegando dados, voz e imagem em circuitos de baixa e alta velocidade, vem com uma política amparada pela lei TECNOLOGIA DA INFORMAÇÃO – CÓDIGO DE PRÁTICA PARA GESTÃO DA SEGURANÇA DA INFORMAÇÃO – NBR ISO/IEC 17799 DE AGOSTO 2001 e INSTRUÇÃO NORMATIVA Série INFORMÁTICA NÚMERO 001 REVISÃO 0 DE 12/11/2001.

A segurança da informação é aqui caracterizada pela preservação da confidencialidade para garantir que a informação é acessível somente por pessoas autorizadas a terem acesso; pela Integridade que salvaguarda da exatidão completa da informação e dos métodos de processamento, acesso; pela disponibilidade: garantia de que os usuários obtenham acesso à informação e aos ativos correspondentes conforme seu respectivo perfil.

Cada vez mais as organizações, seus sistemas de informação e redes de computadores são colocados à prova por diversos tipos de ameaças a segurança da informação de uma variedade de fontes, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, fogo ou inundação. Problemas causados por vírus e ataques de hackers cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados. Os controles de segurança da informação são consideravelmente mais baratos e mais eficientes se forem incorporados nos estágios iniciais dos projetos e da especificação dos requisitos.

Esta norma fornece orientações para gestão da segurança da informação para uso por aqueles que são responsáveis pelo suporte, gerência de rede ou manutenção da segurança em suas instalações. Adicionalmente tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre as organizações.

Para os efeitos desta Norma, aplicam-se as seguintes definições:

Segurança da informação e preservação da confidencialidade, integridade e disponibilidade da informação; avaliação de risco: avaliação de risco, impactos e vulnerabilidade da informação e das instalações/equipamentos de processamento da informação e da probabilidade de sua ocorrência; gerenciamento de risco no processo de identificação e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação; backup em que salvaguarda das informações negociais, bases

de dados, sistemas operacionais e outras informações definidas pela política específica para backups.

2.3.1 Política de Backup

Cada Unidade Descentralizada (Sede/Regional) terá um administrador, ou uma equipe de administradores, responsável por backup.

Os backups deverão ser feitos via CD ou Fita DAT ou Fita DLT ou conforme equipamento disponível e periodicamente as fitas/CD devem ser substituídas, mesmo se ainda não tiverem apresentando defeito de leitura ou gravação, pois o desgaste pelo uso também influencia na perda da integridade dos dados.

Nomenclatura dos Backups Full irão ser copiados para a fita todos os arquivos selecionados. Possibilita que a partir dele (Full), sejam feitos backups somente dos arquivos alterados.

O backup diferencial copiará para a fita de backup, todos os arquivos selecionados que tenham sido alterados após a execução de um backup completo (full).

O Backup de Cópia, copiará todos os arquivos selecionados para uma unidade de fita de backup, como cópia de segurança e devem ser armazenadas no prédio de outra empresa, para restauração em caso de sinistro. As cópias de segurança são feitas semanalmente, com o tipo de backup full.

Este funcionamento do Backup se dará diariamente de segunda a Sexta-feira, **incremental**, dos servidores de arquivos.

Diariamente de segunda a sexta-feira, **full**, do Correio Eletrônico, via Backup NT e dos servidores Banco de dados, conforme software disponível para backup. Nos Sábado o backup será full com todos os servidores de arquivos. No domingo o backup será full dos servidores banco de dados. As cópias serão guardadas na Sala-Cofre da **CEL** para formar o backup semanal e o backup de quatro sábados em quatro semanas consecutivas do mês vigente, constituirá o backup mensal, que por sua vez, a última fita do último sábado de cada mês será guardada na Sala-Cofre da **CEL** e uma cópia na Sala-Cofre da **CEB** complementando o backup mensal que se englobará em doze backups mensais para organizar o backup anual.

2.3.2 Política de Acesso Remoto

A **CEL** (Sede/Brasília) é o ponto de entrada para intranet;

A Superintendência de Tecnologia da Informação – CELTI, de Brasília é responsável pelo cadastramento de usuários para acesso remoto - 0800; Todo acesso remoto deverá ser solicitado via e-mail para a Área de Superintendência de Tecnologia da Informação – CELTI;

Compete a Área de Superintendência de Tecnologia da Informação – CELTI, a monitorar os acessos via **0800 e RAS**;

Compete a Área de Superintendência de Tecnologia da Informação – CELTI, criptografar todos os protocolos direcionados para o servidor de acesso aos recursos liberados para internet;

Qualquer recurso que o(s) usuário(s) deseja(m) disponibilizar no servidor mencionado no item 3.2 deverá solicitar por escrito à Área de Superintendência de Tecnologia da Informação – CELTI;

Compete a Área de Superintendência de Tecnologia da Informação – CELTI, a aceitar ou disponibilizar outra forma de acesso.

Compete a Área de Superintendência de Tecnologia da Informação – CELTI, monitorar todos os recursos do servidor de acesso.

2.5 Auditoria de Hardware

Em relação aos aplicativos utilizados, é de fundamental importância avaliar a performance da máquina E10K seu tempo de resposta e o impacto das alterações na nova plataforma computacional. É importante também avaliar implementação de facilidades no novo ambiente, Levantando junto a empresas do setor com mesma plataforma a analisar impactos de upgrade de aplicativos mantendo contato com as demais equipes para qualquer alteração a ser processada no ambiente.

Seu banco de dados Oracle é utilizado acompanhando o crescimento de table space seu planejamento de necessidades de espaço em disco suas estatísticas de uso de recursos do ORACLE, para implementar melhorias, seu log e ocupação de espaço; um estudo de análise de packages e patches corretivos e quando for o caso implantar com novas versões/releases e por fim acompanhar performance e tempo de resposta, avaliando a adequação de memória e área de swap.

Com o uso do sistema UNIX se faz necessário a avaliação da segurança e integridade do ambiente, observando a performance e tempo de resposta, disponibilidade 24 horas x 7 dias com suas futuras atualizações em packages e patches do sistema operacional.

Da mesma lógica a rede da sede é constantemente monitorada, observando a performance, tempo de resposta e disponibilidade.

2.6 Auditoria de Software

A *CEL* tendo várias Regionais (8) com muitas Localidades e conseqüentemente com muitos usuários, foi necessário a criação de um grande número de perfis de autorização por módulo componente do R3, pois todos querem ter independência e segurança dos dados atualizados de sua respectiva Regional.

Participação da Auditoria desde o início da implementação do sistema é muito importante, identificando os Módulos mais críticos (Ex.: PM), e acompanhando os mesmos de modo efetivo e com foco voltado as reais necessidades da empresa. Os critérios para concessão dos acessos ao R3 devem ser verificados quanto as reais necessidades de cada colaborador que atua(m) no(s) Módulo(s) e devem ser autorizados pela Gerencia imediata do funcionário e pelo responsável(eis) do(s) Módulo(s).

No ambiente de produção os acessos aos Perfis com poderes totais no sistema: SAP_ALL e SAP_NEW deverão ser suprimidos para efeito de segurança do próprio ambiente produtivo, nem mesmo o Suporte ao R3 (Basis) deverá te-lo.

A centralização das responsabilidades do processo de implementação na informática (TI) e nos Gestores dos Módulos:

Autorizar e determinar os componentes das equipes de implementação (áreas de negócios, auditoria, informática e consultores externos);

Treinar os usuários envolvidos na implementação;

Efetuar documentação padronizada e devidamente aprovada da customização dos Módulos do sistema; Após implementação, determinar os responsáveis pela criação dos perfis (Basis) com regras escritas. Para uma maior segurança, segregar os ambientes (Servidores), isto é, a implementação deve ser feita observando a independência dos domínios no(s) servidor(es) (*Landscape*): Servidor de Desenvolvimento; Servidor de *Quality & Assurance (Revisão Projeto)* e Servidor de Produção. Este software efetua a varredura em todos os servidores componentes da NETCEL diagnosticando suas vulnerabilidades e classificando-as por grau de prioridade sugerindo a correção a ser efetuada nos mesmos.

Este relatório será posteriormente enviado pela Equipe de Segurança aos responsáveis pela administração da Hardware: E10000 (UNIX), Software: R3 (Basis) e REDE (NETCEL) onde estes deverão atuar na correção das vulnerabilidades de maior grau. Periodicidade de entrega do Relatório: Bimestral.

3. Conclusão

A Segurança da Informação nas organizações é um requisito gerencial de extrema importância visto que atualmente o valor agregado da informação está cada vez mais em evidência. Por este motivo, quanto mais seguro for o ambiente computacional de uma empresa tanto maior será sua credibilidade no mercado e também seu diferencial competitivo. Atualmente as organizações estão cada vez mais investindo no chamado Office Security, formando e especializando gerentes na área de Segurança da Informação visando a sua diferenciação e evitando com isso perdas que possam ocorrer e provocar prejuízos irreparáveis tanto administrativos quanto financeiros.

No caso de uma organização geradora e distribuidora de Energia Elétrica a segurança da área de manutenção de equipamentos de geração de energia é essencialmente a parte vital da empresa. O plano de segurança desta área deve ser detalhado e especialmente divulgado nos âmbitos de toda empresa pois precisa ser conhecido por todos envolvidos nesta manutenção. No caso de uma falha o Plano de Contingência inserido neste contexto deve ser acionado rapidamente com o objetivo de evitar danos na vida das pessoas e empresas que usufruem da energia que no mundo moderno é nada menos que fundamental.

O módulo PM regido pelo sistema SAP R/3 é de fundamental importância para a empresa Centrais Elétricas Light. Na medida em que permite a manutenção do seu pleno funcionamento e distribuição de energia elétrica para as suas subsidiárias. Por se tratar de um ambiente extremamente crítico com funcionamento de 24 horas e 7 dias por semana foi estabelecido um alto grau de contingência de rede, hardware, software e auditoria para este módulo com total atenção em suas equipes. Estas equipes proporcionam total suporte com práticas bem definidas e imediatas para possíveis acidentes ou paradas ocasionais deste sistema, de forma que esta equipe conta com um pessoal bastante especializado e conhecedor não só do módulo em questão mas de uma abrangência a todo sistema que envolve o SAP R/3.

Diante de toda esta realidade os gerentes de segurança devem estar preparados e treinados para os imprevistos e deve basear suas ações no Plano de Segurança criado na própria empresa. O grande desafio é planejar e gerenciar este Plano de Segurança. Não é um trabalho fácil, requer uma equipe comprometida e dedicada para avaliar cada canto de toda organização, buscando falhas nos processos, erros não detectáveis na área de S.I. E não fica por aí, o trabalho se expande para a segurança física, a segurança dos acessos à empresa, os riscos ambientais, riscos de sabotagem e até mesmo políticos às quais a organização possivelmente possa estar sujeita.

O planejamento apenas não basta. Criar um plano perfeito, baseado nas normas da ISO 17799, criar as normas específicas da empresa, todo Plano de Contingência, todos os itens abordados se ficarem guardados na gaveta de nada adiantará todo este trabalho. O Plano de Segurança deve ser gerenciado de forma eficaz e acima de tudo auditado de tempos em tempos verificando de toda organização está assimilando os conceitos já definidos e reciclando conhecimento para possíveis inovações que surgirem.

Referências

[Dias, Cláudia, 2000] – Dias, Cláudia . “Segurança e Auditoria da Tecnologia da Informação” . Axcel Books do Brasil, 2000.

Manuais do R3 – Elaborados pela SAP Brasil, 2000

Manuais da SUN/ Unix /Solaris, 2000

Normas Técnicas da CEL – Centrais Elétricas Light

NBR ISO/IEC 17799 – ABNT – Associação Brasileira de Normas Técnicas, Agosto 2001.

www.abnt.org.br