

OUTRAS APOSTILAS EM:
www.projetoderedes.com.br

**FACULDADE PITÁGORAS DE TEIXEIRA DE FREITAS
CURSO DE CIÊNCIA DA COMPUTAÇÃO**

**GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM REDES DE
COMPUTADORES**

Julian Mayer Rigo
Wellington Paulino Oliveira

**TEIXEIRA DE FREITAS
2009**

OUTRAS APOSTILAS EM:
www.projetoderedes.com.br

JULIAN MAYER RIGO
WELINGTON PAULINO OLIVEIRA

GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Trabalho de Conclusão de Curso
apresentado ao Colegiado de Ciência da
Computação para obtenção do título de
Bacharel em Ciência da Computação pela
Faculdade Pitágoras.

Orientador: Prof. Esp. Ramilton Costa
Gomes Júnior

Co-orientadora: Prof^a. Esp. Rose Marie
Mendes de Oliveira

TEIXEIRA DE FREITAS

2009

Dados Internacionais de Catalogação na Publicação (CIP)
(Biblioteca Teixeira de Freitas, BA, Brasil)

R572g

Rigo, Julian Mayer, 1986-

Gestão de segurança da informação em redes de computadores / Julian Mayer Rigo, Welington Paulino Oliveira. – 2009.

74 f.

Orientador: Ramilton Costa Gomes Júnior.

Trabalho de conclusão de curso (graduação) - Faculdade Pitágoras de Teixeira de Freitas, Curso de Ciência da Computação, 2009.

1. Segurança da informação. 2. NBR ISO/IEC 17799. 3. ITIL. I. Oliveira, Welington Paulino. II. Gomes Júnior, Ramilton Costa. III. Faculdade Pitágoras de Teixeira de Freitas. Curso de Ciência da Computação IV. Título.

CDD 005.8

JULIAN MAYER RIGO
WELINGTON PAULINO OLIVEIRA

GESTÃO DE SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

Monografia apresentada ao curso de Ciência da Computação da Faculdade Pitágoras - Unidade Teixeira de Freitas, como requisito parcial para obtenção do título de Bacharel em Ciência da Computação.

Aprovada em 14 de dezembro de 2009.

COMISSÃO EXAMINADORA

Prof. Esp. Ramilton Costa Gomes Júnior
Faculdade Pitágoras – Unidade Teixeira de Freitas
Orientador

Prof. Esp. Thiago Alves Miranda
Faculdade Pitágoras – Unidade Teixeira de Freitas
Avaliador

Prof. Esp. Carlos Alberto Dantas da Costa
Faculdade Pitágoras – Unidade Teixeira de Freitas
Avaliador

AGRADECIMENTOS

Agradeço a **Deus**, fonte da vida e do amor, na certeza de que sem Ele nada seria possível.

Aos meus pais, **Adilson e Graça**, por acreditar e por, muitas vezes, colocar os meus sonhos em primeiro lugar.

Aos meus irmãos, **André e Adriana**, pela paciência nos momentos confusos.

A **Daisy**, pela companhia que sempre me motivou a buscar cada vez mais.

Ao colega **Wellington**, por fazer parte deste trabalho e por ter persistido sempre, até nos momentos mais difíceis.

Enfim, a todos que aceitaram dividir com os livros a minha companhia.

Julian Mayer Rigo

AGRADECIMENTOS

Agradeço primeiramente a **Deus**, pois sem Ele, nada seria possível e não estaríamos aqui reunidos, desfrutando, juntos, destes momentos que nos são tão importantes.

Aos meus pais **José Francisco e Maria Leozina** e á minha amada esposa **Pâmela Cristina** pelo esforço, dedicação e compreensão, em todos os momentos desta e de outras caminhadas.

Em especial, ao meu grande amigo **Julian Rigo**, por sua confiança e credibilidade em minha pessoa e a todos aqueles que, direta ou indiretamente, colaboraram para que este trabalho consiga atingir aos objetivos propostos.

Welington Paulino Oliveira

“A sobrevivência da empresa não é fundamental apenas quanto ao aspecto da rentabilidade. [...] O CPD, como ponto vital de muitos negócios, pode ser o âmago dessa questão. Sua vulnerabilidade pode ser a vulnerabilidade da própria organização. Sua destruição pode equivaler ao fim da própria organização.”

Carlos Caruso & Flávio Steffen

RESUMO

O presente trabalho buscou realizar um estudo sobre a segurança da informação em ambientes corporativos, levando em consideração a expansão das redes de computadores, as conseqüentes vulnerabilidades a que estão sujeitas e o valor que as informações representam para o negócio das organizações. Com base em referenciais teóricos, normas técnicas e *frameworks* de qualidade em gestão de Tecnologia da Informação foi possível identificar algumas ferramentas e técnicas que garantem a segurança das informações. Tais ferramentas foram divididas em três camadas: física, lógica e humana. Cada uma das camadas possui características específicas e são interdependentes. O fato de existir um alto nível de segurança em apenas uma das camadas não garante segurança para as outras. Conforme identificou o estudo, a gestão da segurança da informação deve levar em consideração uma proteção uniforme nos três aspectos, caso contrário, todo o investimento realizado será inútil. Ao analisarmos todas as camadas e realizarmos um estudo nas principais ferramentas de cada um delas, constatamos que a área humana, em especial, é um dos pontos mais vulneráveis de toda a estrutura, conforme afirmam os autores, isso deve-se ao fato de que as empresas simplesmente ignoram o fator humano no processo de informatização, investindo somente em equipamentos e tecnologias. Ao não capacitar pessoas, as empresas acabam abrindo uma brecha na segurança e colocando em risco suas informações, a ignorância ou curiosidade humana é um dos pontos mais explorados pelos atacantes. Finalizamos o estudo buscando formas de evitar que os danos causados por um ataque ou por um desastre natural impactem significativamente nos negócios da empresa, através de uma análise sobre as formas de continuidade dos serviços de TI propostas pelo *framework* ITIL V2.

Palavras-chave: segurança da informação, NBR ISO/IEC 17799, ITIL, camadas, física, lógica, humana.

ABSTRACT

This study attempts to make a study on information security in corporate environments, taking into account the expansion of computer networks, the resulting vulnerabilities of the subject and the value that represents the information for business organizations. Based on theoretical frameworks, technical standards and frameworks for quality management in information technology was possible to identify some tools and techniques that ensure the security of information. Such tools were divided into three layers: physical, logical and human. Each layer has specific characteristics and are interdependent. The fact that there is a high level of security in one of the layers does not guarantee security for others. As the study identified, the management of information security must take into account a uniform protection in three ways, otherwise the entire investment will be useless. By analyzing all layers and to perform a study on the main tools each of them, we find that the human area, in particular, is one of the most vulnerable of the whole structure, as the authors say, this is due to the fact that companies simply ignore the human factor in the process of computerization, investing only in equipment and technology. By failing to train people, companies end up leaving a gap in security and endangering their information, ignorance or human curiosity is one of the most exploited by attackers. We conclude the study looking for ways to prevent the damage caused by an attack or a natural disaster significantly impacting the company's business, through an analysis of the forms of continuity of IT services framework proposed by ITIL V2.

Keywords: Information Security, ISO / IEC 17799, ITIL, Layers, Physics, Logic, Humana.

SUMÁRIO

INTRODUÇÃO	10
1. SEGURANÇA DA INFORMAÇÃO	12
1.1 NORMAS DE SEGURANÇA	13
1.2 SEGURANÇA EM CAMADAS	14
2. SEGURANÇA FÍSICA	16
2.1 ESTRUTURA FÍSICA E LOCALIZAÇÃO	16
2.2 ENERGIA ELÉTRICA	19
2.3 CABEAMENTO	21
2.4 CLIMATIZAÇÃO	22
2.5 PROTEÇÃO CONTRA INCÊNDIO	22
3. SEGURANÇA LÓGICA	24
3.1 FIREWALLS	24
3.2 ANTIVÍRUS	25
3.3 SEGREGAÇÃO DE REDES	28
3.4 CONTROLE DE ACESSOS DE USUÁRIOS	30
3.5 MONITORAMENTO	30
3.6 CRIPTOGRAFIA	32
3.7 BACKUP	34
4. SEGURANÇA HUMANA	35
4.1 SEGURANÇA EM RECURSOS HUMANOS	35
4.2 DOCUMENTAÇÃO DE PROCEDIMENTOS	37
4.3 POLÍTICAS DE TI	38
4.4 TREINAMENTOS E CONSCIENTIZAÇÃO	39
5. GERENCIAMENTO DE CONTINUIDADE DOS SERVIÇOS DE TI	41

5.1 ANÁLISE DE IMPACTOS E AVALIAÇÃO DE RISCOS	41
5.2 ESTRATÉGIAS DE CONTINUIDADE	43
5.3 PLANO DE CONTINGÊNCIA	44
CONSIDERAÇÕES FINAIS	47
REFERÊNCIAS.....	49
GLOSSÁRIO	51
ANEXOS	55

INTRODUÇÃO

A informação, na sociedade contemporânea, é um dos ativos mais valiosos para as corporações, as empresas passaram a utilizar essas informações como diferencial competitivo, para ganhar mercado e para aumentar a produtividade das suas fábricas, criando assim, uma enorme dependência com relação aos seus dados. Somam-se a este cenário a grande expansão das redes de computadores nos últimos anos e, a distribuição geográfica das empresas em torno do mundo, elevando a necessidade de estarem cada vez mais conectadas com filiais, escritórios e parceiros. Esta combinação resulta no aumento das vulnerabilidades as quais o ambiente corporativo está sujeito e a necessidade constante de aprimoramentos do setor de Tecnologia da Informação, a fim de reduzir os riscos para o negócio.

Acompanhando este processo, empresas e órgãos públicos ligados a Tecnologia da Informação vêm desenvolvendo normas técnicas e melhorando suas práticas para garantir a segurança das informações corporativas. Além disso, busca-se capacidade de dar continuidade ao negócio mesmo quando ocorrem falhas graves, seja um ataque *cracker*¹, uma pane, ou até mesmo um desastre natural.

No que diz respeito às formas de segurança, podemos citar a segurança física: voltada à estrutura material da tecnologia, como por exemplo, sistemas de proteção contra incêndio e a climatização do *Datacenter*². A segurança lógica: trata de *softwares* (*firewalls*, antivírus) e arranjos lógicos na organização das redes de computadores. E por último, mas não menos importante, apresenta-se a segurança operacional (humana), que visa estipular normas de utilização a serem seguidas pelas pessoas envolvidas em todo o processo tecnológico corporativo, sejam usuários leigos ou profissionais de TI.

¹ Diferentemente dos ataques *hackers*, o ataque *cracker* é aquele que visa roubo ou danos às informações.

² Local onde ficam concentrados os servidores e equipamentos de maior criticidade para o negócio da empresa.

Desta forma, completa-se uma estrutura de segurança multicamadas (Física, Lógica e Operacional), as quais são regidas por normas de qualidade como a NBR ISO/IEC 17799:2005, NBR 11515 e por *frameworks*³ de gerenciamento de serviços de TI como ITIL e COBIT.

Como podemos notar, esta é uma área com abrangência muito grande, portanto o nosso trabalho focará em mostrar os recursos disponíveis e não irá se aprofundar na explicação sobre a utilização dessas ferramentas.

Temos por tanto, uma questão a responder: Como garantir uma segurança física, lógica e humana eficaz para as redes de computadores e *Datacenters*?

Com a ajuda das normas da Associação Brasileira de Normas Técnicas (ABNT), da Biblioteca de Infra-Estrutura de TI (ITIL), em conjunto com as contribuições dos referenciais teóricos e práticos pretendemos esclarecer os principais pontos relacionados à gestão de segurança da informação em redes de computadores.

Este trabalho está dividido em cinco capítulos. No primeiro, estaremos fazendo uma explanação sobre o que é segurança da informação, e como ela tem evoluído desde os primórdios da humanidade aos dias atuais, como as normas de segurança e a segurança em camadas possibilitam uma proteção adequada às informações. No segundo capítulo será abordada a segurança física em um *Datacenter*, segundo a norma de qualidade NBR ISO/IEC 17799 de 2005. No terceiro capítulo abordaremos a segurança lógica necessária para que uma rede de computadores esteja segura. No quarto capítulo, fecharemos a tríade de segurança explanando sobre a segurança humana, a qual irá apontar alguns procedimentos a serem adotados no que diz respeito às pessoas. O quinto e último capítulo trata sobre o gerenciamento de continuidade dos serviços de TI conforme o *framework* ITIL, e culminará em uma explanação sobre o Plano de Recuperação de Desastres (*Disaster Recovery Plan*), comumente conhecido como Plano de Contingência.

³ Modelo de trabalho e ferramentas pré-definido

1. SEGURANÇA DA INFORMAÇÃO

O processo de proteção da informação das ameaças a sua integridade, disponibilidade e confidencialidade, caracteriza-se como Segurança Informação. (BEAL, 2005). Está claro que vivemos numa sociedade em que a informação nunca foi tão valorizada como é hoje, CARUSO & STEFFEN (2006) afirmam que o bem mais valioso de uma empresa pode não ser o produto fabricado por seus operários ou o serviço prestado ao cliente, mas as informações relacionadas a esse bem de consumo ou serviço.

Ao longo da história, o homem sempre buscou dominar o conhecimento sobre o mundo que o cercava. Nos primórdios, ter informações úteis significava a sobrevivência em meio a um ambiente radicalmente hostil. Com o passar do tempo e com o avanço tecnológico, as formas de registro das informações foram sendo alteradas, o que antes era armazenado apenas na memória dos indivíduos, passou a ser registrado através de símbolos com o surgimento dos primeiros alfabetos.

Como o fato de possuir informações poderia tornar algumas pessoas mais poderosas do que outras, o acesso às informações sempre foi restrito. Para CARUSO & STEFFEN (2006, p. 24), “os primeiros suportes para o registro de informações foram as paredes das habitações humanas”, que por si já demonstravam algum tipo de segurança, limitando o acesso aos habitantes ou a pessoas próximas.

Atualmente, não há organização humana que não seja altamente dependente da tecnologia da informação (CARUSO & STEFFEN, 2006), com o advento da informática, a utilização dos computadores pessoais e a abertura comercial da *internet*⁴, a quantidade de informações nunca foi tão grande e concentrada no mesmo lugar.

A norma NBR ISO/IEC 17799 (2005, p. ix) afirma que a Segurança da Informação é:

⁴ Rede mundial de computadores.

“Especialmente importante no ambiente dos negócios, cada vez mais interconectado. Como um resultado deste incrível aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades”.

Todo ambiente tecnológico precisa dispor de métodos e ferramentas de proteção das informações. A segurança obtida através de meios técnicos é limitada, por isso deve ser apoiada por uma gestão e por procedimentos adequados. (NBR ISO/IEC 17799, 2005).

Para SÊMOLA (2003), o resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco pontos principais:

- **Confidencialidade:** Somente as pessoas autorizadas terão acesso às informações;
- **Integridade:** As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados;
- **Disponibilidade:** O acesso às informações sempre que for necessário por pessoas autorizadas;
- **Autenticidade:** Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio;
- **Legalidade:** Garante que as informações foram produzidas respeitando a legislação vigente.

Estes são os cinco pilares da segurança da informação, conhecidos como C.I.D.A.L., eles nos ajudam a identificar os pontos que devem ser levados em consideração sempre que é necessário manipular ou armazenar informações.

1.1 NORMAS DE SEGURANÇA

Diante do risco crescente que há em torno dos ambientes informatizados, empresas e organizações do mundo todo criam e aperfeiçoam soluções para segurança. Dentre as soluções, estão as normas de qualidade voltadas à segurança das informações, como é o caso da ISO 17799 publicada em dezembro de 2000 pela

International Organization for Standardization (Organização Internacional para Padronização). Devido ao interesse em tal norma, a ABNT (Associação Brasileira de Normas Técnicas) publicou em 2001 a versão brasileira, intitulada NBR ISO 17799 – Código de Prática para a Gestão da Segurança da Informação. Em setembro de 2005 a norma foi revisada e publicada como NBR ISO/IEC 17799:2005. Hoje, a norma NBR ISO/IEC 17799:2005 compõe uma família de normas sobre gestão de segurança da informação, nomeada como 27000.

SÊMOLA (2003) afirma que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que dêem uniformidade a um processo, produto ou serviço.

Em paralelo às normas, estão os *frameworks* de qualidade e gestão de serviços de TI, como ITIL e COBIT. Estes possuem características menos rigorosas quanto à aplicação dos conceitos, já que são classificados como “Melhores Práticas”. O responsável pela análise pode adaptar o *framework* ou utilizar apenas os processos que mais lhe interessam. Diferente das normas de qualidade ISO, onde o analista tem a obrigatoriedade de implantar os controles exatamente de acordo com o padrão estipulado, caso contrário estará fora das conformidades.

O *framework* ITIL foi desenvolvido em 1980, pelo governo britânico, com o objetivo de melhorar os processos realizados pelo departamento de TI do próprio governo. (BON, 2005). A partir da sua criação, muitas empresas, entre elas Microsoft, IBM e HP, perceberam que poderiam melhorar seus processos utilizando o ITIL. Tornando-se, de fato, um padrão utilizado por todo o mundo.

1.2 SEGURANÇA EM CAMADAS

Para SÊMOLA (2003), a gestão de segurança da informação pode ser classificada em três pontos: tecnológica, física e humana. É muito comum organizações se preocuparem apenas a área tecnológica, focando em antivírus⁵, *Firewalls*⁶, e esquecerem-se dos outros aspectos que também estão envolvidos no processo. SÊMOLA (2003) afirma ainda, que a todo momento as empresas são alvos de

⁵ Verificar capítulo 3.2.

⁶ Verificar capítulo 3.1.

ataques nesses três aspectos com o objetivo de identificar o ponto mais fraco para uma investida contra a segurança. Como grande parte das empresas deixa a área física e humana de lado, esses se tornaram os pontos mais frequentes dos ataques registrados.

Uma pesquisa realizada no ano de 2000 pelo CSI (*Computer Secure Institute*), em parceria com o FBI (*Federal Bureau of Investigation*), mostrou que 100% das empresas entrevistadas possuíam *softwares* antivírus instalados nos computadores, porém, na mesma pesquisa, 85% disseram que foram vítimas de infecções por vírus. Em outra questão, 91% dos entrevistados responderam ter *Firewalls* instalados em suas redes, entretanto, 30% das empresas foram vítimas de invasões e 55% tiveram problemas com acessos não autorizados originados por funcionários. A pesquisa foi realizada entre os anos de 1998 e 2000 nos Estados Unidos e contou com a participação de 512 empresas de diversos setores de negócio.

Fica claro que houve investimento em tecnologia, mas outros fatores foram negligenciados. Ao término da pesquisa foi ressaltada a necessidade de um melhor treinamento dos usuários e funcionários das empresas com relação à utilização das ferramentas de segurança, bem como a criação de políticas de segurança. ADACHI (2004) distribui as camadas de segurança em física, lógica e humana, esta será a classificação tomada como base para o desenvolvimento deste trabalho.



Figura 1: Representação da divisão da segurança em camadas.

2. SEGURANÇA FÍSICA

Conforme dispõe a norma NBR ISO/IEC 17799 (2005, p.46), o projeto de implantação de um *Datacenter* deve contemplar uma série de características únicas, de forma que “sejam projetadas e aplicadas proteção física contra incêndios, enchentes, terremotos, explosões, perturbações da ordem pública e outras formas de desastres naturais ou causados pelo homem.”

De forma geral podemos colocar algumas considerações iniciais:

- Materiais inflamáveis não devem ser armazenados perto das áreas onde se pretende proteger;
- Os equipamentos de contingência e mídias de *backup*⁷ devem ficar armazenados em outro local, distante o suficiente para que, se caso houver um desastre natural, estes não sejam afetados juntamente com o local de armazenamento principal;
- O local protegido deve contar com materiais de detecção e combate a incêndio.
- Controle de acesso de pessoas ao *Datacenter* deve ser extremamente rigoroso, o trabalho nessas áreas deve ser sempre supervisionado.

2.1 ESTRUTURA FÍSICA E LOCALIZAÇÃO

A estrutura física contempla os quesitos de engenharia e arquitetura da construção do prédio. Deve-se levar em consideração os seguintes pontos:

Assoalho, teto e paredes – A forma ideal de assoalho a ser utilizado é o piso elevado, pois vem a facilitar:

1. A passagem de cabos de dados e de energia elétrica;
2. A distribuição das linhas de comunicação;
3. A remoção rápida, caso necessário;

⁷ Cópias de segurança.

4. Pode servir como meio para a instalação de dispositivos contra incêndio;
5. E pode funcionar como *Plenum* de insuflamento de ar condicionado⁸.

CARUSO & STEFEN (2006) afirmam que o piso deve ser elevado numa altura de 0,2m a 0,4m, podendo chegar a 0,6m caso sejam utilizados equipamentos de grande porte. Se o insuflamento de ar condicionado for uma opção utilizada, deve-se prever o uso de placas perfuradas ou grelhas para a passagem do ar. A estrutura metálica que sustenta o piso deve ser aterrada para que não haja risco de descargas elétricas e possíveis danos aos equipamentos.



Figura 2: Instalações internas do Datacenter. Fonte: <http://www.acecoti.com.br>

O teto deve ser de material resistente, fixado por estruturas metálicas de material não inflamável e que não desprenda partículas. Deve ser dada preferência a estruturas elevadas para que possibilite a passagem de cabos elétricos e de dados, instalação do sistema de combate a incêndio e grelhas para o ar-condicionado. (CARUSO & STEFFEN, 2006). Deve ainda ser resistente o suficiente para permitir a instalação de luminárias, grelas, sensores e outros acessórios caso seja necessário. Neste quesito, o acabamento também deve ser impecável para que não haja vazamentos, pode-se utilizar uma camada impermeável que, caso ocorra, o vazamento não chegue a causar danos dentro do ambiente de tecnologia.

⁸ O piso nesse caso serve como uma câmara onde o ar frio é novamente elevado, tornando a distribuição do ar mais homogênea no ambiente.

As paredes devem ser de concreto ou alvenaria, capazes de suportar impactos ou furacões. O ambiente não deve possuir janelas ou outras aberturas, somente uma porta corta-fogo, o conjunto deve garantir no mínimo uma hora de resistência ao fogo a uma temperatura de 1260° C. A iluminação deve contribuir com a segurança e a produtividade do ambiente. De preferência utilizar luminárias fluorescentes com índice de iluminação não inferior a 500 lux⁹ medidos a 1m do piso, deve ser evitado ofuscamento da visão, pontos escuros, bem como reflexo nos monitores. Caso algum equipamento utilizado no *Datacenter* tenha recomendações específicas de iluminação estas devem ser contempladas, de modo que não interfira no funcionamento dos equipamentos presentes na sala.

As paredes serão o meio para a fixação de placas de indicativas sobre tensão das tomadas, regiões reservadas à passagem de cabos, local de equipamentos de proteção e caminhos de saída. O acabamento deve proporcionar limpeza e organização ao ambiente, elementos de PVC e cortinas devem ser evitados, assim como carpetes devido ao acúmulo de poeira.

A localização do *Datacenter* deve ser planejada para que as possibilidades de riscos sejam as menores, para tal CARUSO & STEFFEN (2006) afirmam que o edifício, que deve abrigar apenas o *Datacenter*, seja construído em uma área exclusiva, acima do nível do solo e com as instalações mais sensíveis no centro, tendo as áreas de apoio na periferia, seguindo o conceito de camadas concêntricas de segurança.

O edifício não deve ser identificado a fim de dificultar a sua localização por curiosos, somente aqueles que precisarem acessá-lo devem saber a sua localização. (NBR ISO/IEC 17799, 2005). Do ponto de vista interno, a área de operação deve estar em um local separado da área onde estão os equipamentos de processamento de dados. No caso de uma visita, esta primeira sala seria a única a ser mostrada aos visitantes.

⁹ Unidade de medida para luminosidade.

2.2 ENERGIA ELÉTRICA

A energia elétrica fornecida ao *Datacenter* é um dos pontos mais críticos, ela deve ser ininterrupta e limpa, portanto recomenda-se que toda alimentação seja fornecida por um sistema de *no-break*¹⁰ e, posteriormente, dependendo da disponibilidade acordada com os clientes, pode se tornar imprescindível a utilização de geradores a óleo CARUSO & STEFFEN (2006). Além de fornecer energia estabilizada¹¹, este conjunto (*no-breaks* e geradores) atua também como fonte alternativa de energia.

O sistema elétrico deve ser dimensionado para suportar 50% a mais da carga máxima a ser utilizada, devido aos picos de demanda, vislumbrando-se sempre a possibilidade de expansões futuras.

O cabo de entrada de energia proveniente da concessionária deve ser duplicado na subestação, de forma que haja um barramento alternativo de entrada de energia. Este mesmo barramento poderá ser conectado à fonte de energia redundante, no caso um gerador a óleo, obtendo-se assim uma fonte alternativa de acionamento imediato caso a primeira falhe.

Todo o sistema deve contar com um aterramento¹² eficaz, o mais indicado é o aterramento em malha com o uso de várias barras de cobre. Isto evita o risco de choques acidentais aos operadores e também a perda de informações em mídias magnéticas ou ópticas.

Os esquemas abaixo mostram dois modelos de estruturas redundantes:

¹⁰ Equipamento de proteção que fornece energia estável e ininterrupta por meio de um conjunto de baterias.

¹¹ Corrente alternada onde não há variação na intensidade.

¹² Técnica onde parte da instalação é conectada ao solo evitando prejuízos aos equipamentos em caso de descargas atmosféricas e outros transientes.

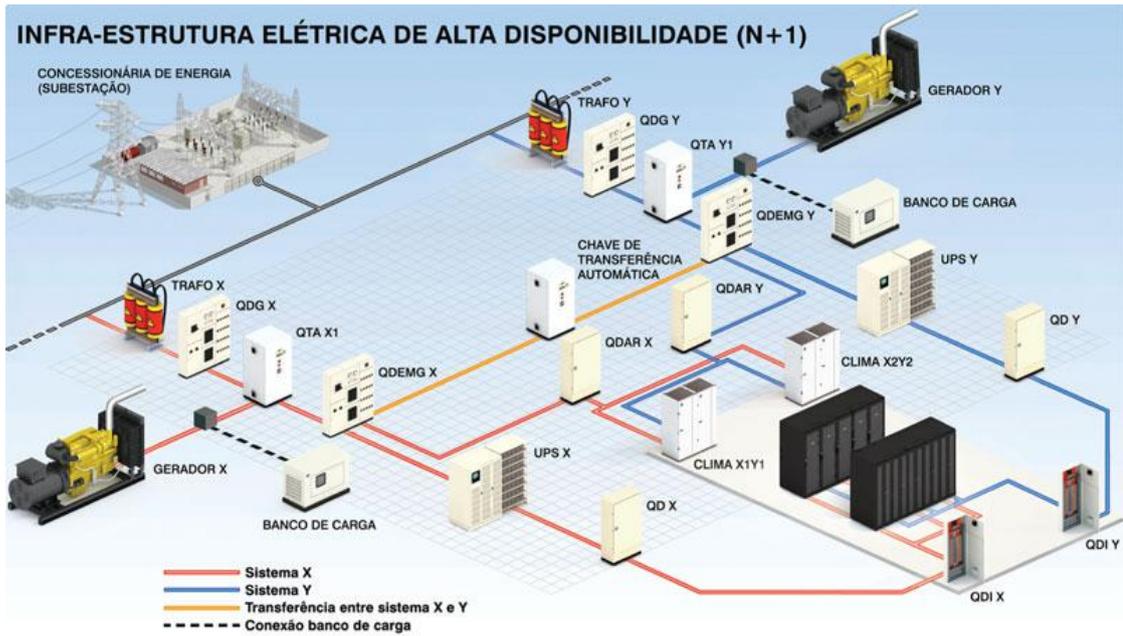


Figura 3: Esquema de Rede Elétrica Redundante N+1. Fonte: <http://www.acecoti.com.br>.



Figura 4: Esquema de Rede Elétrica Duplamente Redundante 2(N+1). Fonte: <http://www.acecoti.com.br>

2.3 CABEAMENTO

A norma NBR ISO/IEC 17799:2005 faz algumas recomendações a respeito da instalação e manutenção do cabeamento utilizado no *Datacenter*, seja este de dados ou de energia, deve sempre garantir a segurança do serviço em questão.

“Convém que o cabeamento de energia e de telecomunicações que transporta dados ou dá suporte aos serviços de informações seja protegido contra interceptação ou danos.” (NBR ISO/IEC 17799, 2005, p.34).

A separação dos cabos de dados e de energia é uma medida contra a interferência que pode ocorrer devido aos campos eletromagnéticos que corrente elétrica gera. Alguns outros pontos podem ser levantados em conformidade com a norma supracitada:

1. As linhas de transmissão quem entram nas instalações de processamento da informação sejam subterrâneas, sempre que possível, ou recebam uma proteção alternativa adequada;
2. O cabeamento de redes seja protegido contra interceptações, evitando trajetos que passem por vias públicas;
3. Nos cabos e nos equipamentos sejam utilizadas marcações claramente identificáveis, a fim de minimizar erros no manuseio;
4. Seja utilizada uma lista de documentação das conexões para reduzir a possibilidade de erros;
5. Utilização de blindagem eletromagnética para a proteção alternativa dos cabos;
6. Realização de varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos;
7. Acesso controlado aos painéis de conexão e as salas de cabos.

Sempre que os serviços sejam taxados como “críticos”, deve-se analisar a possibilidade de utilizar fibra óptica. Apesar do custo elevado, este tipo de meio de transmissão é muito menos suscetível a falhas e apresenta uma velocidade bastante elevada com relação aos cabos de par trançado. (TANEMBAUM, 2003)

2.4 CLIMATIZAÇÃO

Este ponto é muito importante para um *Datacenter*, porém não é levado a sério por algumas empresas. O fato é que muitos equipamentos dependem de instalações de climatização para funcionarem corretamente. Um sistema de condicionamento de ar destina-se a conservar níveis de temperatura e umidade adequados, estáveis e, ainda é primordial, manter o ambiente isento de impurezas. Para impedir a entrada de poeira e fumaça pode-se utilizar a técnica de manter a pressão positiva dentro do recinto.

A temperatura e a umidade relativa do ar devem ficar em torno de 22° C e 55% respectivamente. CARUSO & STEFFEN (2006) propõem uma tolerância de 10% para a temperatura e 5% para a umidade, porém deve ser respeitado um limite de alteração na temperatura de no máximo 1° C a cada 5 minutos, e de 45% a 55% para a umidade relativa em 8 horas.

Para garantir a eficiência do sistema de climatização é aconselhável o insuflamento de ar. Como sabemos, o ar frio concentra-se na parte inferior do ambiente, utiliza-se então, um conjunto de tubulações para conduzir o ar frio para a parte superior novamente. Desta forma haverá uma melhor utilização do ar frio e conseqüentemente melhor refrigeração do *Datacenter*.

2.5 PROTEÇÃO CONTRA INCÊNDIO

Nos outros tópicos deste capítulo, tentamos, sempre que possível, lembrar que os materiais utilizados no *Datacenter* devem ser anti-chamas e não combustíveis, isso evita muito a propagação de incêndio caso aconteça. Porém, esta medida serve apenas para evitar que o fogo se alastre muito rapidamente e não seria suficiente para conter um foco de incêndio. Os sistemas de detecção de incêndio têm evoluído muito nos últimos anos, em áreas sensíveis como o *Datacenter*, é recomendado o uso de detectores de fumaça e detectores de câmaras de aspiração que podem diagnosticar um incêndio através da análise do ar com raios *laser*. A ABNT possui

uma norma específica para sistemas de detecção e alarme de incêndio, a NBR 9441. Uma das regulamentações dessa norma é a distância entre os sensores, que devem ser instalados no piso, teto e paredes do ambiente.

O combate ao incêndio pode ser automático, através da interconexão do sistema de detecção com a liberação de gases¹³ para a extinção do fogo, ou manual, com a liberação do gás extintor por um comando ou ainda, pelo uso de extintores de CO₂ que devem ser alocados em número e local adequados dentro do recinto. Extintores de água ou pó químico devem ser evitados, devido aos danos que podem causar a equipamentos eletrônicos. Caso a opção escolhida seja o combate automático por gás, deve-se evitar o uso do gás carbônico (CO₂), pois quando utilizado em larga escala, provoca uma mudança brusca na temperatura do ambiente, podendo também comprometer a integridade dos equipamentos.

Conforme a norma NBR 9441, as paredes do *Datacenter* devem suportar uma temperatura de no mínimo 1260° C por uma hora. Portas com propriedade corta-fogo são extremamente recomendadas também.

¹³ O gás recomendado é o FM200, que não é tóxico para as pessoas e muito eficaz na extinção do fogo.

3. SEGURANÇA LÓGICA

3.1 FIREWALLS

Com o avanço das redes de computadores e a possibilidade de conectar praticamente qualquer computador a outro, um grande problema surgiu aos administradores de rede, a possibilidade de um intruso acessar uma rede privada se passando por um usuário legítimo e ter acesso a informações sigilosas. (CARUSO & STEFFEN, 2006). Além disso, conforme TANEMBAUM (2003), existe ainda o problema dos vírus e *worms*¹⁴, que podem burlar a segurança e destruir dados valiosos.

Para ajudar a manter as redes mais seguras, os *Firewalls* remetem à idéia de uma única passagem para os dados, onde todos são analisados antes de serem liberados e, de fato, o que acontece é exatamente isso, todo o tráfego de uma rede passa obrigatoriamente por uma estação de controle para ser analisado, caso não encontre nenhuma restrição, o *Firewall* libera o pacote e este segue para seu destino, caso contrário, é sumariamente descartado.

CARUSO & STEFFEN (2006, p. 218) afirmam que:

“Normalmente, um Firewall é instalado no ponto de interligação de uma rede interna com a Internet. Todo o tráfego, nos dois sentidos, tem de passar por este ponto e, dessa forma, atender aos requisitos da política de segurança da instalação.”

O administrador da rede pode definir políticas específicas para a filtragem do tráfego da rede, por exemplo, pode indicar que todo o tráfego endereçado para a porta 23¹⁵ seja bloqueado. Desta forma o atacante, ao enviar pacotes de fora da rede para a porta 23, será automaticamente ignorado pelo destino e ainda, o administrador poderá ser alertado sobre a tentativa.

¹⁴ Pragas digitais que se propagam pela rede fazendo cópias de si mesmos e infectando outros computadores.

¹⁵ Na porta 23 é executado o serviço de Telnet, o qual permite que uma série de funções sejam realizadas à distância, entre elas o acesso remoto a um computador.

O *Firewall* se divide em dois componentes: o filtro de pacotes, que faz exatamente a função exemplificada acima, inspecionando cada pacote de entrada e saída, e identificando a origem e o destino de cada um. E o *gateway* de aplicação que, conforme TANEMBAUM (2003), em vez de apenas examinar os pacotes brutos, o *gateway* toma a decisão de transmitir ou descartar a mensagem através da análise dos campos de cabeçalho, do tamanho da mensagem e até do seu conteúdo (em busca de palavras-chave). Esta última situação é bastante útil quando se deseja bloquear o acesso a conteúdos que não têm uma fonte específica, ou que são providos por um serviço onde as portas são atribuídas dinamicamente. Neste caso os pacotes passariam pelo filtro de pacotes, porém seriam bloqueados pela análise do *gateway* de aplicação.

Muitos *Firewalls* já identificam os ataques antes que consigam causar algum dano sério. Porém, um dos ataques mais comuns e que ainda é a causa de muitas indisponibilidades de serviços é o ataque de negação de serviço (DoS), onde o atacante envia milhares de pedidos de conexão ao servidor, que por sua vez responde a cada um deles, normalmente cada pedido fica retido por um tempo até que seja eliminado automaticamente pelo servidor, porém, até que isso aconteça o limite de conexões do servidor pode ser excedido, e a partir daí nenhuma conexão nova poderá ser aceita, deixando o serviço em questão indisponível para outros usuários. Para se proteger contra esse ataque o *Firewall* deve ser configurado para limitar a quantidade de conexões estabelecidas por cada usuário, desta forma, mesmo que o atacante utilize vários endereços de origem diferentes para conseguir várias conexões, será mais trabalhoso conseguir a negação do serviço para usuários legítimos.

3.2 ANTIVÍRUS

Os vírus de computador se tornaram uma praga no mundo digital e as empresas têm gasto milhares de Dólares na busca por formas de combatê-los. Basicamente um vírus é um código malicioso que se hospeda em outro programa do computador. Segundo TANENBAUM & WOODHULL (2000), quando um programa infectado é

iniciado, este começa uma varredura no disco rígido em busca de outros arquivos executáveis, quando um programa é localizado, ele é infectado anexando-se código do vírus no final do arquivo e substituindo a primeira instrução por um salto para o vírus. Desta maneira, toda vez que o usuário tenta executar um programa infectado, irá, na verdade, executar o código do vírus e estará, cada vez mais, propagando o código malicioso para outros arquivos. Além de infectar outros programas, um vírus tem controle quase que total sobre a máquina e pode fazer muitas coisas no computador, como apagar, modificar ou bloquear arquivos do usuário, exibir mensagens na tela e, muito comumente, pode simplesmente danificar o setor de inicialização do disco rígido, impossibilitando o funcionamento do Sistema Operacional. A única alternativa para o usuário neste caso é reformatar o disco rígido e recriar o setor de inicialização.

Combater um vírus não é uma tarefa fácil (TANEMBAUM, 2003), principalmente devido ao fato de que ele pode ter embutido em seu código uma característica de mutação própria, transformando-se novamente em uma estrutura desconhecida pelo antivírus. CIDALE (1990) cita quatro formas diferentes de detecção possíveis para antivírus:

- **Escaneamento de vírus conhecidos:** Apesar de ser bastante antigo, este ainda é o principal método de detecção de códigos maliciosos. Assim como, na área da saúde, os médicos e infectologistas precisam conhecer parte do vírus (biológico) para desenvolver uma vacina que será aplicada em humanos, na área computacional, as empresas desenvolvedoras dos antivírus (digitais) precisam também conhecer o código malicioso para poder criar uma vacina e proteger os computadores. Uma vez que as empresas recebem o vírus, uma parte do código é separada (*string*¹⁶) e tomada como “assinatura” ou impressão digital do vírus, que por sua vez, passa a integrar uma lista de vírus conhecidos. Esta lista é distribuída por meio de atualizações via *internet* para os computadores pessoais. A partir daí, sempre que o antivírus identificar em um programa a *string* de um vírus, este será bloqueado.

¹⁶ Conjunto de caracteres sequenciais.

- **Análise Heurística:** Este processo consiste em uma análise, por parte do antivírus, em programas que estão sendo executados em busca de indícios de ações que seriam executadas comumente por vírus. Por exemplo, uma função de escrita em um arquivo executável, ou em vários arquivos executáveis de forma sequencial, isso poderia ser um indício de que um código malicioso estaria tentando se propagar, atribuindo seu código à outro executável. Neste caso a análise Heurística do antivírus deve bloquear a ação e alertar o usuário sobre o evento. Este é um processo complexo e que nem sempre funciona como deveria, conforme CIDALE (1990), algumas funções que seriam identificadas como suspeitas podem ser totalmente normais em determinadas circunstâncias, gerando o que o próprio chama de falso positivo, que é quando um alerta de vírus é dado para um arquivo legítimo.
- **Busca Algorítmica:** Em comparação com o primeiro método, este processo de identificação é um pouco mais preciso, pois utiliza um conceito de busca mais complexo. Uma série de condições pode ser imposta para que o vírus seja identificado, como a extensão do arquivo, o tamanho, a *string*, e outros mais. Devido à sua maior complexidade, torna a pesquisa mais lenta e, por isso, acaba sendo utilizado apenas em casos onde o método de comparação de *string* não é eficaz.
- **Checagem de Integridade:** Diferentemente dos outros métodos, nesta técnica não é necessário conhecer o código do vírus anteriormente para se proteger dele. Consiste basicamente em criar um registro com os dígitos verificadores de todos os programas instalados no computador, TANENBAUM (1999) afirma que tal registro deve ser feito logo após uma formatação completa e armazenado em um local seguro¹⁷ no computador e criptografado. Posteriormente, quando executada uma verificação, o código verificador do programa em execução será comparado com o código armazenado no banco de dados do antivírus, caso haja alguma alteração significa que o programa foi alterado sem permissão. Tal abordagem não impede a infecção, mas permite detectar cedo a sua presença.

¹⁷ Tem-se como local seguro, onde existam poucas permissões ao usuário. Dificultando a gravação não autorizada.

Como podemos perceber nenhum dos métodos disponíveis até hoje é completamente eficaz contra as pragas virtuais. O mais certo é utilizar um antivírus que esteja sempre atualizado e que possua métodos de detecção próprios eficientes como a Análise Heurística e a Checagem da Integridade, mesmo assim, deve-se sempre instalar *softwares* originais e de fontes confiáveis (TANEMBAUM, 1999).

3.3 SEGREGAÇÃO DE REDES

A norma NBR ISO/IEC 17799 (2005) afirma, em um dos seus controles, que um método de controlar a segurança da informação em grandes redes é dividi-la em domínios de redes lógicas diferentes. De fato, esta é uma prática comum em redes de computadores estruturadas que garante acesso restrito a certos serviços. Por exemplo, uma instituição de ensino como uma faculdade, que possui laboratórios de informática utilizados por seus alunos, não seria conveniente que eles estivessem desenvolvendo suas pesquisas na mesma rede onde se encontra o servidor de banco de dados com suas notas, faltas e vida financeira. Tais dados poderiam estar em risco. Porém, também não seria conveniente para a instituição manter uma infraestrutura física separada para atender apenas aos laboratórios, isso sairia caro, portanto com a divisão lógica da rede é possível manter apenas uma estrutura física impondo limites logicamente.

“Tal perímetro de rede pode ser implementado instalando um gateway seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informação entre os dois domínios. Convém que este gateway seja configurado para filtrar tráfego entre estes domínios e bloquear acesso não autorizado conforme a política de controle de acesso da organização”. (NBR ISO/IEC 17799, 2005, p. 74).

Outra situação onde a segregação de rede se faz necessária é quando máquinas da rede precisam receber acessos externos, como é o caso de servidores *Web*¹⁸ e *e-mail*, por exemplo. O fato de deixá-las no mesmo segmento de rede de outras máquinas não impediria que o serviço que elas executam funcionasse corretamente, porém, em caso de invasão todo o segmento de rede estaria em risco. O atacante poderia se utilizar de uma falha no servidor *Web* para ter acesso ao servidor de

¹⁸ Servidores de hospedagem de sites.

banco de dados da empresa e roubar informações sigilosas, além é claro, de ter controle sobre o primeiro servidor.

Neste caso, seria criada uma divisão lógica, ou uma sub-rede, chamada de DMZ (Zona Desmilitarizada). Este segmento seria protegido por um *Firewall*, porém, permitiria o acesso de clientes externos conforme demandam os seus serviços.

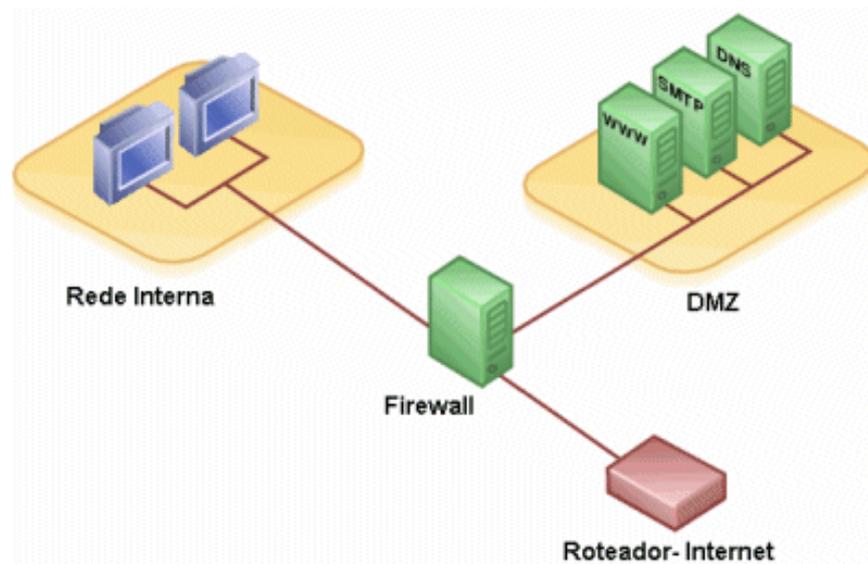


Figura 5: Segregação de rede com uma DMZ. Fonte: <http://www.projetoderedes.com.br>.

Segundo SÊMOLA (2003), o conceito de *Firewall*, e que se aplica muito bem nessa situação, está ligado às paredes internas de uma construção que impedem que o fogo se propague de uma sala para outra. Caso o atacante consiga explorar uma falha em um dos serviços da DMZ, ainda não teria acesso à rede interna da corporação. A recomendação da norma NBR ISO/IEC 17799 (2005, p. 73) é que “os domínios sejam definidos de acordo com uma análise de riscos e requisitos de segurança diferentes”. Esta análise pode determinar a divisão da rede em vários segmentos, como sistemas publicamente acessíveis, redes internas e ativos críticos¹⁹.

¹⁹ Podemos considerar como ativos críticos aqueles que possuem dados sigilosos da empresa ou que representam alto grau de dependência à continuidade dos negócios.

3.4 CONTROLE DE ACESSOS DE USUÁRIOS

O objetivo do controle de acessos de usuário é controlar o acesso à informação. (NBR ISO/IEC 17799, 2005). CARUSO & STEFFEN (2006) afirmam que o controle de acessos leva em consideração, basicamente, duas questões que devem se responder antes de qualquer coisa:

- Quem irá acessar?
- Quais recursos serão acessados?

Essas duas questões irão gerar um inventário com todos os usuários e os recursos disponíveis no ambiente da empresa. Conhecendo os usuários, deve-se organizá-los em grupos por departamentos ou por funções relacionadas. A seguir, os direitos de acesso devem ser dados por pessoas autorizadas de dentro da empresa. “Convém que exista um procedimento formal de registro e cancelamento de usuário para garantir e revogar acessos em todos os sistemas de informação e serviços”. (NBR ISO/IEC 17799, 2005, p.66).

Vários usuários poderão receber as mesmas designações de acesso às informações, por isso, devem ser agrupados em entidades, e as permissões atribuídas à entidade, facilitando o gerenciamento dos privilégios.

3.5 MONITORAMENTO

O monitoramento das atividades em um ambiente de tecnologia da informação tem como objetivo principal detectar atividades não autorizadas realizadas por usuários internos ou externos. (NBR ISO/IEC 17799, 2005). O registro das atividades deve ser feito de forma automática pelos sistemas, gerando um arquivo chamado de *log*. Este arquivo deve ser protegido contra falsificação e acesso não autorizado, mantendo a sua integridade e confiabilidade caso seja necessário utilizá-lo. (TANEMBAUM, 1999).

Muitos dos *logs* gerados trazem informações referentes não só aos acessos de usuários, mas também, informações técnicas referentes aos recursos do sistema. Essas informações podem ser úteis na resolução de problemas, pois muitos sistemas emitem alertas sobre deficiências encontradas na execução de tarefas. Desta forma registros de *log* geralmente contêm um grande volume de dados, tornando difícil para uma pessoa identificar eventos importantes. Por tanto, a norma NBR ISO/IEC 17799:2005 recomenda o uso de ferramentas de auditoria para a análise adequada desse material.

Alguns sistemas, como o *Microsoft Windows Server 2003*, por exemplo, possuem uma ferramenta de análise de *logs* própria, que em caso de eventos considerados relevantes envia uma mensagem para o administrador informando sobre o problema.

As atividades de todos os usuários (administradores ou operadores) devem ser registradas sejam estas realizadas em um sistema operacional ou em um *software* ERP²⁰. CARUSO & STEFFEN (2006) definem alguns dados como indispensáveis em um *log*:

- Identificação do usuário;
- Data, horário;
- Informações sobre o evento;
- Identificação do terminal utilizado.

O monitoramento pode ser feito não só através de *logs*, mas, também em tempo real, como é o caso dos sistemas de monitoramento de serviços. Basicamente, o administrador tem acesso às condições de operação de um ativo mesmo este estando em uso, seja um *software* ou *hardware*. E através da emissão de relatórios²¹ é possível identificar problemas, planejar melhorias ou, definir regras para uma melhor utilização da ferramenta.

²⁰ Sigla para *Enterprise Resource Planning*. Sistema que integra grande parte das operações de uma empresa.

²¹ Verificar anexo D.

3.6 CRIPTOGRAFIA

Com a vulnerabilidade dos mecanismos de comunicação utilizados atualmente sempre existe a possibilidade de interceptação dos dados trafegados. CARUSO & STEFFEN (2006, p. 172) afirmam que “enquanto as linhas de comunicação fizerem uso de sinais elétricos para a transmissão de sinais, elas continuarão a ser vulneráveis à penetração não autorizada”. Isso se deve ao fato de que interceptar um sinal elétrico é muito simples e pode ser difícil de identificar o intruso.

Como muitas vezes é impossível garantir a confiabilidade do meio de transmissão, passou-se a utilizar uma técnica para esconder a mensagem caso esta fosse interceptada durante o trajeto. A palavra criptografia tem origem grega, significa "escrita secreta", esta técnica já é utilizada a milhares de anos. (TANEMBAUM, 1999). Consiste basicamente na substituição ou transposição de caracteres de uma mensagem.

O emissor criptografa o texto utilizando um padrão estabelecido pela chave de cifragem e envia a mensagem ininteligível. Chegando ao destino, o texto cifrado precisa ser descifrado, realizando o processo inverso, e seguindo o mesmo padrão estabelecido pelo emissor. As chaves de cifragem dividem-se em simétricas e assimétricas.

Na criptografia simétrica a chave utilizada para cifrar uma mensagem é a mesma utilizada para voltar ao texto inteligível (CARUSO & STEFFEN, 2006). Neste caso o destinatário deve conhecer a chave utilizada pelo emissor para efetuar a troca. É um processo simples, muito utilizado pela maioria dos algoritmos, porém não muito seguro, já que se a chave for descoberta qualquer um poderá ler a mensagem cifrada. (CARUSO & STEFFEN, 2006). Um exemplo claro deste tipo de chave é a Cifra de César²², onde cada letra da mensagem é substituída por outra do alfabeto, seguindo um número de troca de posições. Por exemplo, utilizando uma troca de quatro posições, a letra A seria substituída pela letra E, a letra B seria F e assim por diante. Juntamente com a mensagem cifrada, o emissor deve encontrar um meio de

²² Tem esse nome em homenagem a Júlio César, que utilizava este tipo de cifra para enviar ordens militares ainda na antiguidade.

informar ao destinatário qual a chave para descriptografar a mensagem. Nesse caso, o número de troca precisa ser informado.

Já na criptografia assimétrica, a chave usada para criptografar não pode ser usada para reverter o processo; isto só é possível com uma chave complementar. (CARUSO & STEFFEN, 2006). Um dos poucos exemplos que temos é o método de chaves públicas RSA²³. Este método é baseado em cálculos com números primos, e se utiliza da dificuldade de fatorar tais números. Teoricamente, é perfeitamente possível quebrar a chave RSA, porém matemáticos têm tentando fatorar números extensos há pelo menos trezentos anos e o conhecimento acumulado sugere que o problema é extremamente difícil. (TANEMBAUM, 1999). Na prática o algoritmo funciona da seguinte forma: primeiro um dos indivíduos (A) que participará da comunicação cria uma chave pública e envia para o outro indivíduo (B), na verdade estará enviando o algoritmo de encriptação. Depois A deve criar a chave privada que será conhecida apenas por ele próprio. B poderá enviar mensagens para A através da chave pública, porém apenas A terá a chave privada para fazer a leitura da mensagem. CARUSO & STEFFEN (2006) fazem uma analogia comparando a chave pública como um cadeado e a chave privada como a chave do cadeado, todos podem fechá-lo, porém só um terá a chave para abri-lo. TANEMBAUM (1999) deixa claro que quanto maior for o número criptográfico escolhido pelo emissor, maior será a dificuldade em quebrar o algoritmo, de fato, a fatoração de um número de 500 dígitos levaria 10^{25} anos. Em contrapartida, maior também, será o tempo gasto no processo de encriptação, o que às vezes, pode não ser satisfatório.

CARUSO & STEFFEN (2006) prevêem que a única forma de quebrar a criptografia RSA, e todas as outras técnicas de chave assimétrica, seria com a entrada de operação dos computadores quânticos:

“Esses computadores terão velocidade de processamento milhões de vezes mais rápida do que os atuais computadores mais rápidos. Por possuírem (por enquanto teoricamente) a capacidade de realizar cálculos simultâneos, isso eliminaria a atual segurança de métodos de chave assimétrica, como o RSA, podendo realizar ataques de força bruta quase que instantaneamente.” (CARUSO & STEFFEN, 2006, p. 182).

Com base nisso, uma nova etapa em algoritmos de segurança está surgindo, será a criptografia quântica. Ao invés de utilizar métodos matemáticos para a geração de

²³ São as iniciais de três estudiosos que criaram o método (Rivest, Shamir, Adleman).

chaves, o novo conceito fará uso das propriedades físicas baseadas na mecânica quântica. Esta já é uma tecnologia conhecida nos laboratórios de pesquisa, entretanto, ainda sem perspectiva de uso a curto prazo, devido principalmente aos altíssimos custos envolvidos do processo de desenvolvimento.

3.7 BACKUP

O processo de *backup* consiste na realização de cópias de segurança de arquivos ou configurações.

A norma NBR ISO/IEC 17799 (2005, p. 48) afirma que o objetivo da realização de *backups* é “manter a integridade e disponibilidade da informação e dos recursos de processamento de informação”. Para tanto, a norma ainda trás alguns itens que devem ser considerados durante o processo:

- Definição da necessidade das cópias;
- Produção de registros das cópias efetuadas com documentação²⁴ apropriada;
- As cópias de segurança sejam armazenadas em uma localidade remota com um nível apropriado de segurança;
- As mídias sejam testadas regularmente para garantir que elas são confiáveis;
- Em caso de confidencialidade dos dados, as cópias sejam criptografadas.

Devem ser feitas cópias de segurança de todos os trabalhos desenvolvidos nas estações dos usuários. CARUSO & STEFFEN (2006, p. 194) afirmam que “essa providência facilita a recuperação das informações, precavendo-se de algum dano ou sinistro nos arquivos originais”. Conforme SÊMOLA (2003), várias cópias do mesmo arquivo podem ser feitas, dependendo da sua criticidade para a continuidade dos negócios.

²⁴ Verificar anexo A;

4. SEGURANÇA HUMANA

Das três camadas, esta é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual (SCHNEIER, 2001).

A gestão desta camada envolve mais do que *software* e *hardware*, equipamentos e programas só estarão vulneráveis caso algo seja negligenciado ou configurado de forma incorreta, ao contrário das pessoas que, comumente executam ações e colocam dados em perigo mesmo sabendo que isso pode trazer sérios danos para a empresa. Educar as pessoas é o maior desafio num ambiente tecnológico. (CARUSO & STEFFEN, 2006).

4.1 SEGURANÇA EM RECURSOS HUMANOS

Segundo a norma de qualidade NBR ISO/IEC 17799 (2005), deve-se levar em consideração três momentos referentes aos recursos humanos em uma corporação:

- Antes da contratação;
- Durante a execução das funções;
- Encerramento das atividades profissionais.

O primeiro momento trata da seleção e avaliação dos candidatos a uma determinada vaga na empresa. É preciso tornar claro ao futuro colaborador qual será a sua função, quais as responsabilidades atribuídas ao seu cargo, verificar se este aceita e, se possui um perfil de acordo com as regras definidas. Esta etapa resulta em um documento contendo a descrição das funções profissionais, as responsabilidades relativas à segurança da informação corporativa, e as ações a serem tomadas em caso de desrespeito aos requisitos de segurança.

A norma NBR ISO/IEC 17799 (2005, p.13), afirma que:

“Acordos de confidencialidade e de não divulgação protegem as informações da organização e informam aos signatários das suas responsabilidades, para proteger, usar e divulgar a informação de maneira responsável e autorizada.”

A idéia principal é que todos na organização tenham conhecimento sobre suas responsabilidades e regras da mesma, para que possam executar tarefas de forma consciente.

No segundo momento, a execução das funções, deve-se estar atento fundamentalmente na educação e treinamento das práticas de segurança (SÊMOLA, 2003). Após se comprometer a seguir corretamente a política e o regimento da empresa, as pessoas precisam ser instruídas sobre como fazer isso. Para tal, o usuário deve receber treinamento adequado sobre os mecanismos de segurança utilizados dia-a-dia e sobre recomendações de boas maneiras de uso.

SÊMOLA (2003) cita o compromisso que a direção da empresa deve ter com a segurança e afirma que a direção não deve apenas solicitar a adoção das diretrizes de segurança, e sim mostrar na prática o cumprimento da política de segurança pelo alto escalão da empresa, assegurando que todos tenham consciência de suas responsabilidades.

Caso o usuário, mesmo tendo conhecimento de suas responsabilidades, negligencie a segurança de forma evidente, pode-se fazer uso de um processo disciplinar contra o autor (NBR ISO/IEC 17799, 2005). É importante que a medida tomada seja justa e clara, tornando o processo transparente para os demais funcionários.

O último momento é quando o funcionário deixa a empresa ou ocorre uma mudança nas suas funções, alterando também o nível que este acessa as informações corporativas. O usuário primeiramente deve perder o acesso aos recursos que não irá mais utilizar, caso esteja apenas mudando de função, deverá ser definido pelo gestor da informação quais serão os novos acessos desde funcionário e quem ficará responsável pelas informações que deixaram de ser gerenciadas por ele. É importante também que os bens de informação que estão de posse do usuário que está sendo desligado, sejam devolvidos ou repassados a outras pessoas autorizadas dentro da empresa, como é o caso de *notebooks*²⁵, *smartphones*²⁶ e

²⁵ Computador portátil.

outros ativos. Esta medida garante que as informações contidas nesses equipamentos não sejam utilizadas para outros fins fora da empresa.

Devido à natureza nem sempre racional do ser humano, e apesar dos esforços em *firewalls*, encriptação e etc, este ainda é o elo mais fraco na tríade da segurança da informação (SÊMOLA, 2003).

4.2 DOCUMENTAÇÃO DE PROCEDIMENTOS

A complexidade dos ambientes de TI exige que todos os procedimentos realizados sejam oficializados e registrados de forma clara e precisa. Isso contribui para que nenhuma tarefa seja realizada de forma incorreta ou que, simplesmente, seja esquecida pelo operador. “Convém que os procedimentos de operação sejam documentados, mantidos atualizados e disponíveis a todos os usuários que deles necessitem.” (NBR ISO/IEC 17799, 2005, p.40).

Dentre outras recomendações, a norma NBR ISO/IEC 17799 (2005) afirma que os procedimentos de operação documentados especifiquem as instruções para cada uma das tarefas, incluindo:

- Processamento e tratamento da informação;
- Rotinas de *Backup*²⁷;
- Agendamentos de tarefas²⁸;
- Instruções para tratamento de erros e incidentes;
- Dados para contatos de suporte em caso de dificuldades técnicas e eventos operacionais inesperados;
- Informações sobre configuração e funcionamento de sistemas;
- Procedimentos para início e recuperação em caso de falha do sistema.

²⁶ Aparelho celular com funções avançadas.

²⁷ Verificar anexo A.

²⁸ Verificar anexo B.

Tais documentos devem ser tratados como regras formais, é recomendado que as mudanças nos procedimentos sejam autorizadas pela direção da empresa (SÊMOLA, 2003).

CARUSO & STEFFEN (2006) definem os procedimentos operacionais como “o estabelecimento de padrões de execução de atividades e de comportamento de seres humanos”. Deve-se tomar cuidado na operacionalização desses procedimentos, pois o fato de manter rotinas pode torná-los mecânicos e repetitivos perdendo o sentido principal. Por isso, convém lançar mão de recursos como rodízio de pessoal, cursos de reciclagem e mudanças superficiais nos procedimentos, com o objetivo de manter as equipes responsáveis atentas.

4.3 POLÍTICAS DE TI

Segundo CARUSO & STEFFEN (2006, p. 53), “Política de segurança é um conjunto de diretrizes gerais, destinadas a governar a proteção a ser dada a ativos da companhia”. Conforme a norma NBR ISO/IEC 17799 (2005), uma política de segurança pode ser dividida em três pontos, facilitando a sua elaboração: processual, tecnológico e humano.

Na área Processual, o objetivo é formalizar os processos de segurança da informação na empresa, além da responsabilidade dos usuários com relação aos ativos de tecnologia da informação.

Na área Tecnológica, são definidos os aspectos relevantes ao bom funcionamento dos recursos tecnológicos, como servidores, estações de trabalho, arranjos lógicos, etc. Segundo SÊMOLA (2003), muitos, erroneamente, vêem nesta área a responsabilidade de toda a segurança da empresa, porém isso deve ser bem dividido entre as três áreas em questão, de forma que é inútil manter *softwares* de segurança se os usuários não sabem como utilizá-los.

O fato de existirem processos formalizados e informações tecnológicas sobre o funcionamento dos ativos, não significa que os processos serão seguidos, nem que as configurações serão utilizadas pelas pessoas.

Por isso, a terceira área, trata do aspecto humano, definindo a conduta considerada adequada para a empresa. SÊMOLA (2003, p. 68) diz que:

“Procedimentos e instruções deverão estar presentes na política em maior quantidade por seu perfil operacional, onde é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta do uso de informações”.

Não basta, por exemplo, citar na política que as senhas utilizadas pelos usuários devem satisfazer requisitos de complexidade adequados de acordo com a confidencialidade das informações, deve-se considerar que o usuário pode desconhecer como criar uma senha segura, e ainda outros descuidos que podem ocorrer.

Do ponto de vista estratégico, podemos perceber que as normas são a operacionalização das diretrizes que são definidas pela direção da empresa. Conforme SÊMOLA (2003), as diretrizes têm um papel estratégico, precisam expressar a importância que a empresa dá para a informação. É imprescindível a participação da diretoria neste processo pelo caráter oficial que a política deve ser apresentada aos colaboradores e fornecedores.

Para que uma política seja realmente efetiva, deve-se fazer uso de ferramentas de monitoramento constante. É preciso ainda manter a política sempre atualizada e refletindo as reais necessidades e realidade da empresa, adaptando-a às novas tecnologias, às mudanças administrativas e a novas ameaças (CARUSO & STEFFEN, 2006).

4.4 TREINAMENTOS E CONSCIENTIZAÇÃO

A maioria das empresas não possui uma cultura de segurança da informação, isso dificulta muito a implantação de regras e normas para o acesso a informação. Neste

caso, CARUSO & STEFFEN (2006, p. 61) afirmam que “deve-se estabelecer uma política educacional com relação à segurança, para convencer e obter apoio, antes de introduzir medidas de segurança”. Tendo conhecimento adequado, a eficácia de uma política de segurança é muito maior, além disso, todos os usuários serão, de certa forma, responsáveis pela segurança, já que não podem alegar desconhecimento das normas. Conforme SÊMOLA (2003), “somente desta forma as empresas terão, em seus funcionários, aliados na batalha de redução e administração dos riscos”.

A política de segurança não deve ser um documento de gaveta, servindo apenas como um descargo de consciência do gestor de TI, ele deve ser divulgado, distribuído em forma de cartilhas²⁹, incentivado. Todos devem, não somente saber que ele existe, mas devem praticá-lo como se fosse parte de suas ações cotidianas e naturais. “O fator surpresa é um dos pontos nevrálgicos dos processos de segurança que dependem das pessoas.” (SÊMOLA, p. 129, 2003).

Os treinamentos podem ser feitos de diversas formas, de acordo com o público alvo na empresa, como seminários, palestras, cursos de capacitação e certificação, termos de responsabilidade e outras mais. Colocando o funcionário como peça chave de uma engrenagem muito maior, e tornando-o consciente de sua posição na empresa, é possível que este passe a se comprometer com a segurança, pois começa a entender os riscos dos seus atos. A idéia é fazer os usuários compreenderem que apenas um fato isolado pode comprometer toda a segurança da empresa.

²⁹ Verificar anexo C

5. GERENCIAMENTO DE CONTINUIDADE DOS SERVIÇOS DE TI

O gerenciamento de continuidade tem por missão garantir que o negócio da empresa não seja afetado, ou pelo menos minimizar os impactos, caso ocorra um desastre. Para tal é criado um Plano de Continuidade de Serviços de TI, ou Plano de Contingência que estabelece uma série de procedimentos padronizados que devem ser iniciados logo após o acontecimento de um desastre. “O plano de continuidade deve ser projetado com objetivo claro de contingenciar situações e incidentes de segurança” (SÊMOLA, 2003, p.98).

Uma vez que as empresas estão se tornando cada vez mais dependentes da TI para a realização das suas atividades, o impacto causado por uma indisponibilidade das informações e serviços torna-se fatal para muitas corporações. SÊMOLA (2003) afirma que o plano de continuidade deve funcionar como um pára-quedas reserva, após a falha do pára-quedas principal e apesar do susto, a vida do pára-quedista será mantida sem nenhum dano.

5.1 ANÁLISE DE IMPACTOS E AVALIAÇÃO DE RISCOS

Conhecido pela sigla BIA (*Business Impact Analysis*), a Análise de Impactos Sobre o Negócio é a primeira etapa fundamental para a criação de uma estratégia de continuidade. O objetivo é levantar o grau de relevância entre os processos que farão parte do escopo de contingência do plano de continuidade. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que serão necessários para a execução dos processos, para então apurar os impactos que poderiam ser gerados com a paralisação de cada um.

Segundo o *framework* ITIL V2, o resultado que uma empresa pode sofrer com uma interrupção ou desastre pode ser avaliado através da identificação dos processos críticos ao negócio, e a previsão da perda que pode ser causada para a organização com a interrupção desses processos críticos.

Quanto custaria para uma rede varejista, por exemplo, se o processo de vendas ficasse paralisado durante uma hora? Nesse caso é possível visualizarmos claramente a perda financeira, porém há também as perdas imensuráveis, como a imagem que a empresa mantém perante seus clientes e fornecedores, esta também seria avariada com uma paralisação em suas operações. A credibilidade e a confiabilidade da empresa estariam em jogo.

PROCESSOS DE NEGÓCIO	PN1	PN2	PN3	PN4	PN5
ESCALA					
1 NÃO CONSIDERÁVEL					X
2 RELEVANTE	X				
3 IMPORTANTE			X		
4 CRÍTICO				X	
5 VITAL		X			

Tabela 1: Relevância entre processos. Fonte: SÊMOLA (2003, p. 86)

Após identificar os processos críticos na organização entramos em uma etapa chamada de Avaliação dos Riscos. Esta atividade irá analisar a probabilidade de um desastre ou interrupção ocorrer, e definir qual será a extensão da vulnerabilidade na organização.

Enquanto a Análise de Impactos se preocupa com os resultados que uma paralisação pode gerar a empresa, a Avaliação de Riscos irá focar no elemento causador da paralisação. Esta avaliação pode ser dividida em duas etapas, conforme afirma o ITIL V2:

- **Análise de Riscos:** Irá identificar os possíveis riscos, analisando as vulnerabilidades e ameaças para todos os ativos críticos.
- **Gerenciamento de Riscos:** Identificará os contra-recursos para manter os riscos sobre controle. São as ações que deverão ser tomadas para reduzir a probabilidade ou até impedir que a empresa fique em situação de risco.

Ameaças Consideradas

	Incêndio	Greve	Interrupção de Energia	Ataque DoS	Sabotagem	Tolerância
PN1	X		X		X	48 Horas
PN2	X					5 Horas
PN3	X	X	X	X		24 Horas
PN4				X	X	15 Minutos

Tabela 2: Ameaças a serem consideradas no plano de contingência. Fonte: SÊMOLA (2003, p. 94)

Desta forma todos os ativos de TI devem ser avaliados e suas ameaças catalogadas para que a empresa não seja surpreendida com uma vulnerabilidade não conhecida.

5.2 ESTRATÉGIAS DE CONTINUIDADE

Para a definição de um Plano de Recuperação de Desastres (*Disaster Recovery Plan*) é preciso analisar qual estratégia é mais adequada para a empresa. O *Framework* ITIL V2 trás algumas opções:

- **Nenhuma Contingência:** Geralmente quando a Análise de Riscos sugere que a falha dos serviços de TI não afeta o negócio de forma irreparável, esta escolha pode ser feita. De qualquer forma o ITIL afirma que esta opção deve ser documentada deixando claro que, em caso de desastre não haverá nenhum Plano de Contingência disponível.
- **Procedimentos Administrativos:** Caso o custo de uma recuperação seja muito alto, pode-se tomar decisões administrativas para contornar o problema. Um exemplo pode ser o de voltar a utilizar formulários de papel.
- **Estratégia de Fortificação:** Neste caso, toda a estrutura será reforçada para que em caso de desastre a empresa possa continuar utilizando a mesma estrutura. Nada pode dar errado, caso contrário não haverá nenhum outro plano.
- **Arranjos Recíprocos:** É feito um acordo entre duas empresas, onde uma emprestará sua infra-estrutura para a outra caso seja necessário. É possível também que duas empresas mantenham uma área externa independente

para uso em caso de desastres. Esta alternativa possui uma desvantagem com relação à confiabilidade dos dados, já que duas empresas teriam acesso a mesma infra-estrutura.

- **Recuperação Gradual (*Cold Stand-by*):** Neste modelo, a contingência é feita a partir de um ambiente mantido pela empresa com recursos mínimos de infra-estrutura e telecomunicações, para onde recursos de processamento de dados possam ser migrados.
- **Recuperação Intermediária (*Warm Stand-by*):** Neste cenário, haveria um local para a evacuação dos serviços com uma infra-estrutura semelhante ou compatível. Um exemplo desta estratégia são as soluções apresentadas pela IBM e pela SUN *Microsystems* de *Datacenters* montados em *containers*, que podem ser transportados sobre caminhões para o local do desastre. Basta existir um *link* de comunicação e geração de energia para alimentar os equipamentos.
- **Recuperação Imediata (*Hot Stand-by*):** Esta estratégia é recomendada quando a interrupção dos serviços pode afetar a sobrevivência da empresa ou impedi-la de gerar receitas. Geralmente existe um outro ambiente funcionando em paralelo, quando necessário basta redirecionar o *link*³⁰ para o novo local. Muitas vezes esse redirecionamento é feito de forma automática através de um roteador, por exemplo.

5.3 PLANO DE CONTINGÊNCIA

O plano de contingência é produto gerado pelo gerenciamento de continuidade proposto pelo *framework* ITIL V2. Segundo a norma NBR ISO/IEC 17799 (2005, p. 104):

“Convém que os planos sejam desenvolvidos e implementados para a manutenção ou recuperação das operações e para assegurar a disponibilidade da informação no nível requerido e na escala de tempo requerida, após a ocorrência de interrupções ou falhas dos processos críticos do negócio.”

³⁰ Ponto de ligação ou canal de comunicação entre dois locais.

O plano deve esquematizar as ações que serão tomadas para propiciar a continuidade dos serviços essenciais de TI em casos onde as políticas de segurança não foram suficientes para evitar o dano, de forma que a empresa mantenha o mínimo de suas operações em funcionamento. SÊMOLA (2003) afirma que a maioria das empresas entra em colapso muito rapidamente após um desastre no seu ambiente de processamento de dados. Daí a necessidade de manter-se preparado para uma emergência.

CARUSO & STEFFEN apud WEIGHTS (2006) recomenda a adoção de alguns passos para a elaboração do plano de contingência:

1. **Formação da equipe de planejamento:** Deve-se montar uma equipe com representantes das áreas críticas da empresa, as quais não poderiam deixar de funcionar em caso de desastre.
2. **Avaliação das atividades críticas:** Fazendo uso da análise de impactos, a equipe irá fazer um levantamento dos processos críticos do negócio. Neste ponto, podem-se fazer acordos administrativos entre os departamentos da empresa para que facilite o processo de contingência e menos recursos sejam gastos.
3. **Lista do pessoal necessário:** É elaborada uma relação com os nomes, endereços e telefones de todo o pessoal essencial para a execução do plano.
4. **Equipamentos necessários:** Com base nos processos prioritários deve-se dimensionar os equipamentos necessários.
5. **Dados, Software e documentação:** Deve-se tomar providências para manter disponível em caso de emergência, toda a documentação e *softwares* necessários para a restauração dos sistemas.
6. **Alternativas de coleta de dados e distribuição de saídas:** Em caso de emergência a emissão de relatórios e outras saídas podem ser alteradas devido as condições do processamento dos dados. Por isso, deve-se criar alternativas para essas ações.
7. **Acordos de backup em locais alternativos:** Nesta etapa será escolhido o local alternativo para a restauração de toda a estrutura física de processamento. Muitas empresas criam acordos de reciprocidade com outras empresas, ou optam por ter sua própria área de restauração alternativa.

8. **Manuais de contingência:** Todos os procedimentos devem ser registrados rigorosamente e mantidos ao alcance das pessoas responsáveis. Deve-se tomar cuidado com a confidencialidade desse material, pois como conta com informações críticas, este pode servir de guia para sabotagens.
9. **Testes de contingência periódicos:** Na realização dos testes de contingência todos os procedimentos são executados a fim de verificar a sua eficácia. CARUSO & STEFFEN (2006) afirmam que é na realização dos testes que costuma-se encontrar os pontos fracos do plano de contingência.

De nada valem os conceitos contidos no plano de contingência, se a empresa não souber identificar corretamente as suas necessidades. (SÊMOLA, 2003). E acima de tudo, saber prever formas de contornar os possíveis problemas. Para CARUSO & STEFFEN (2006, p. 334) “a vulnerabilidade do centro de processamento de dados pode ser a vulnerabilidade da própria empresa e a sua destruição pode equivaler ao fim da própria organização”.

CONSIDERAÇÕES FINAIS

Estudar sobre a segurança da informação nos fez perceber o quão vasto é o campo da Ciência da Computação e como este se permeia de situações as quais, apenas a lógica e os conhecimentos exatos, não são suficientes para resolver.

As ameaças que uma corporação sofre no mundo real com roubos, sabotagens, desastres, estão na íntegra, presentes no mundo virtual, em forma de invasões, vírus, etc. Em grande parte dos casos, um ataque, seja uma invasão ou um código malicioso que infecta máquinas, pode causar grandes prejuízos, ou até, comprometer temporariamente as operações da empresa. Isto leva a uma crescente demanda de ferramentas, técnicas e profissionais cada vez mais capacitados e cientes de tais ameaças.

A disseminação das redes de computadores possibilitou a troca de informações em velocidade e abrangência nunca antes vistas pela humanidade, por outro lado, trouxe uma gama de ameaças que poderiam comprometer todo o avanço obtido por muitas organizações, isso tem forçado uma mudança na cultura de segurança. Instituições públicas e privadas têm lutado para desenvolver métodos de segurança cada vez melhores com o objetivo de minimizar os riscos envolvidos na manipulação, transmissão e armazenamento de dados.

Uma delas é a norma de segurança NBR ISO/IEC 17799, publicada inicialmente em 2001 e reformulada no ano de 2005 pela Associação Brasileira de Normas Técnicas (ABNT), tem o objetivo de padronizar a operação relacionada a segurança da informação.

A publicação brasileira foi baseada na ISO 17799 internacional, isso reflete uma preocupação mundial neste assunto. Porém, como o custo de implantação de uma norma ISO acaba sendo muito alto para algumas empresas, muitas preferem adotar os *frameworks* de qualidade, que possuem uma versatilidade maior e também conseguem alcançar excelentes resultados. Estes podem ser considerados o início para uma futura adoção da norma ISO. Em nosso trabalho exploramos a norma NBR ISO/IEC 17799:2005 e o *framework* ITIL V2.

Com base nesses métodos e estudos, executamos o nosso estudo focando a gestão de segurança da informação em três camadas: física, lógica e humana. Por meio de referências teóricas com vasta experiência e conhecimento no assunto, tanto da área de Administração, Ciência da Computação e Engenharia, levantamos algumas ferramentas vitais para a segurança. Classificam-se da seguinte forma:

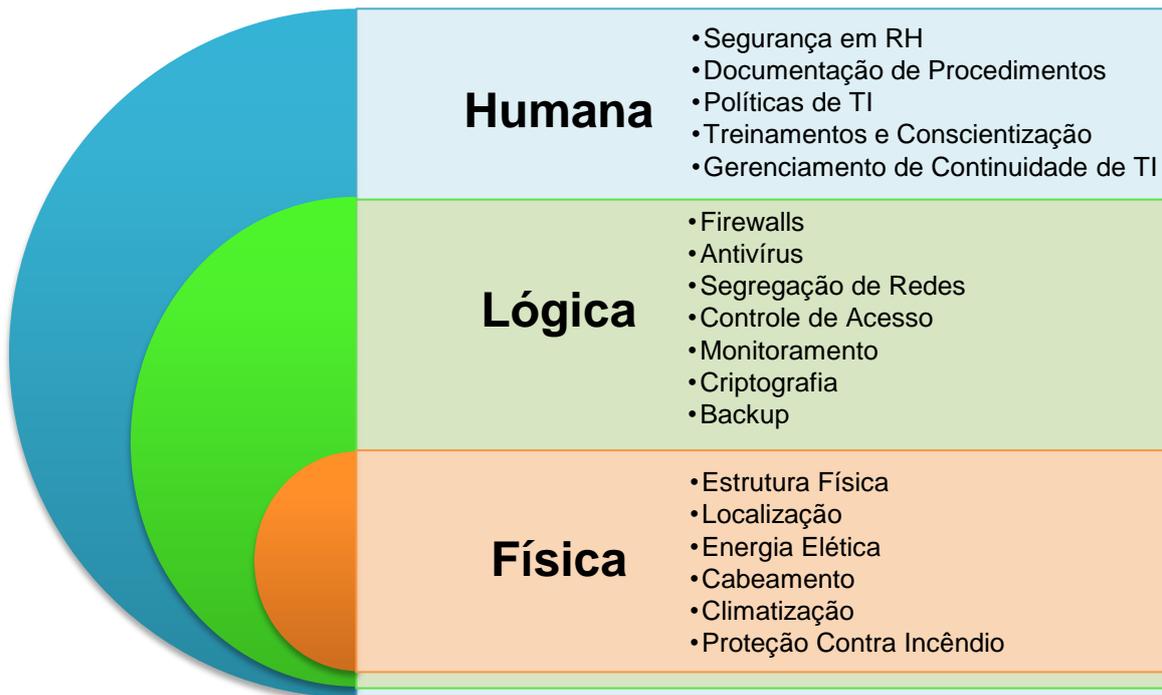


Figura 6: Classificação das ferramentas de segurança em camadas.

A segurança nas camadas física e lógica aparecem como as mais comuns de serem implantadas, pois têm soluções técnicas, muito comum a profissionais na área de tecnologia, porém já na camada humana nem sempre as ações que deveriam garantir a segurança funcionam como esperado. O fator Humano dificulta o controle devido a sua natureza irregular e não previsível.

Cada uma das camadas pode receber muitas outras ferramentas já que a tecnologia está em constante desenvolvimento, assim como as ameaças. E por isso temos a certeza de que o esforço para manter um ambiente corporativo seguro é um trabalho contínuo de atualização e implementação de novos controles, que só deixará de ser realizado quando não houver mais informações a serem guardadas.

REFERÊNCIAS

ACECO TI. **Organização, Segurança e Continuidade**. Disponível em <<http://www.acecoti.com.br>>. Acesso em: 11 ago. 2009.

ADACHI, Tomi. **Gestão de Segurança em Internet Banking** – São Paulo: FGV, 2004. 121p. Mestrado. Fundação Getúlio Vargas – Administração. Orientador: Eduardo Henrique Diniz.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação**. Rio de Janeiro: ABNT, 2005.

_____. **NBR 9441 - Execução de sistemas de detecção e alarme de incêndio**. Rio de Janeiro: ABNT, 1998.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BON, JAN VON. **Foundations of IT Service Management, based on ITIL**. Lunteren - Holanda: Van Haren Publishing, 2005.

CARUSO, Carlos A. A; STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. 3ª Ed. rev. e ampl. São Paulo: Editora Senac São Paulo, 2006.

CIDALE, Ricardo A. **Vírus digital. Uma abordagem para prevenção e manutenção de seus sistemas de informação**. São Paulo: Makron McGraw-Hill, 1990.

CSI/FBI. **2000 CSI/FBI Computer Crime and Security Survey**. Computer Security Institute, Vol.VI, No.1. 2000.

MICROSOFT TECHNET BRASIL. **Academia de Segurança**. Disponível em <<http://www.technetbrasil.com.br/academia2007/seguranca>>. Acesso em: 15 ago. 2009.

SCHNEIER, Bruce. **Segurança.com: segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Editora Campus Elsevier, 2003.

Service Delivery. Londres – Inglaterra: The Stationary Office, 2000.

Service Support. Londres – Inglaterra: The Stationary Office, 2000.

TANEMBAUM, Andrew S; Trad. SOUZA; Vandenberg D. de. **Redes de Computadores**. 4ª Ed. Editora Campus, 2003.

TANEMBAUM, Andrew S; WOODHULL, Albert S; Trad. FURMANKIEWICZ, Edson. **Sistemas Operacionais: Projeto e Implementação**. 2ª Ed. Porto Alegre: Bookman, 2000.

GLOSSÁRIO

ALGORITMO: processo computacional bem definido, baseado num conjunto de regras, finito, que executa uma determinada tarefa.

ANTIVÍRUS: *Softwares* projetados para detectar e eliminar vírus de computador.

ATERRAMENTO: Ligação à terra de todas as partes metálicas não energizadas de uma instalação incluindo o neutro.

BACKUP: É a cópia de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos dados originais.

BANCO DE DADOS: São conjuntos de registros dispostos em estrutura regular que possibilitam a reorganização dos mesmos e produção de informação.

BLINDAGEM ELETROMAGNÉTICA: Uma espécie de escudo protetor que impeça a livre passagem das ondas eletromagnéticas, geralmente feito de metal.

COBIT: *Control Objectives for Information and related Technology*, é um guia de boas práticas apresentado como *framework*, dirigido para a gestão de tecnologia de informação (TI).

CONTAINER: É um equipamento utilizado para transportar carga.

CPD: Centro de Processamento de Dados é o local onde são concentrados os computadores e sistemas confiáveis (*software*) responsáveis pelo processamento de dados de uma empresa ou organização.

CRACKER: É o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética.

DATACENTER: O mesmo que CPD, porém com maior porte.

DISCO RÍGIDO: é o disco interno ao computador onde os dados são armazenados, conhecido também como HD (*hard disk*).

DMZ (ZONA DESMILITARIZADA): É uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a *Internet*.

DOS (DENIED OF SERVICE): Atividade maliciosa onde o atacante utiliza um computador para tirar de operação um serviço ou computador conectado à *Internet*.

E-MAIL: Sistema para troca de mensagens de texto e arquivos de computador via *Internet*.

ERP: São sistemas de informação que integram todos os dados e processos de uma organização em um único sistema.

FIREWALL: Dispositivo de segurança que monitora o tráfego de informação entre uma rede de computadores e a *Internet*.

FRAMEWORK: Modelo de trabalho e disposição de ambientes e ferramentas pré-definidos.

GATEWAY: É uma máquina intermediária geralmente destinada a interligar redes, separar domínios de colisão, ou mesmo traduzir protocolos.

HACKER: Indivíduo com grande conhecimento em informática que consegue romper códigos e senhas e entrar em sistemas exclusivos. É motivado pelo desafio da conquista e não pelo lucro financeiro que o ataque pode trazer.

HARDWARE: Componentes físicos de um sistema de computador, abrangendo quaisquer periféricos como impressoras, modems, mouses.

INSUFLAMENTO: Técnica de elevação do ar frio concentrado na parte inferior de um ambiente.

INTERNET: É um conglomerado de redes em escala mundial de milhões de computadores interligados.

ITIL: *IT Infrastructure Lybrary* é uma biblioteca composta das melhores práticas para Gerenciamento de Serviços de TI.

LINK: Conexão. Seja de dados, telefonia ou energia.

LOG: Registro de atividades gerado por programas de computador.

MICROSOFT WINDOWS SERVER 2003: Sistema operacional de redes desenvolvido pela Microsoft, lançado em 2003.

MÍDIA MAGNÉTICA: É uma mídia de armazenamento não-volátil que consiste em uma fita plástica coberta de material magnetizável.

MÍDIA ÓPTICA: Meios de armazenamento que utilizam tecnologia laser de gravação e leitura.

NO-BREAK: Equipamento destinado a suprir a alimentação elétrica dos equipamentos a ele acoplados, também conhecido pela sigla UPS (Uninterruptible Power Supply).

NOTEBOOK: Computador portátil, leve, designado para poder ser transportado e utilizado em diferentes lugares com facilidade.

PROTOCOLO: É uma convenção ou padrão que controla e possibilita uma conexão, comunicação ou transferência.

REDES LÓGICAS: Segmento de rede distinto através de configurações específicas como faixa de *ip* e máscaras diferentes.

ROTEADOR: Um dispositivo de rede que permite interligar redes distintas

RSA: é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto MIT.

SERVIDOR: É o computador que administra e fornece programas e informações para os outros computadores conectados em rede.

SISTEMA OPERACIONAL: É o programa responsável pelo controle do *hardware* e *software*.

SMARTPHONE: É um telefone celular com funcionalidades avançadas que podem ser estendidas por meio de programas executados no seu sistema.

SOFTWARE: Refere-se aos programas executados no computador.

STRING: Conjunto de caracteres.

TELNET: Protocolo cliente-servidor usado para permitir a comunicação entre computadores ligados numa rede.

TI: Sigla de Tecnologia da Informação.

VÍRUS: Programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando outros programas.

WEB: É o ambiente multimídia *Internet*, também conhecido como WWW.

WORMS: Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador.

ANEXOS

ANEXO A



Documentação de Rede – CPD-TX

TI / Aqui Supermercados

Pág. 13

3. PROCEDIMENTOS

PROCEDIMENTOS AGENDADOS – SERVIDORES			
BACKUP			
SERVIDOR	HORÁRIO	ITENS COPIADOS	DESTINO
Servidor03 (192.168.254.2)	23h	C:\Arquivos de Programas\sc501txt\ C:\Linear\ C:\mysql\ C:\PDVLinx\ C:\SGLinx\ C:\Sitef\	\\servidor02\Suporte\Backups\Backup_ser v03.bkf (192.168.254.10)
Cpd1 (192.168.254.10)	23h	C:\Arquivos de programas\Firebird\ C:\Arquivos de programas\Leucotron Telecom\ C:\Arquivos de programas\Microsoft SQL Server\ C:\Arquivos de programas\TOLEDO\ C:\ATUALIZACAO\ C:\Fotos Produtos\ C:\PDVlinx\ C:\SGLinx\ D:\Drivers\ D:\Programas\ D:\Appserv\	\\servidor01\Backups\Backup_Cpd1.bkf
Servidor01	4h	C:\Arquivos de programas\Microsoft ISA Server\ D:\Configuracao ISA.xml System State	\\servidor03\Backups\Backup_serv01.bkf
Servidor02	3h	C:\distribuicao\ C:\ System volume information\ System State	\\cpd1\Suporte\Backups\Backup_serv02.b kf
DATA DA ÚLTIMA ALTERAÇÃO:			
05/02/2009 07:37			

ANEXO B



Documentação de Rede – CPD-TX

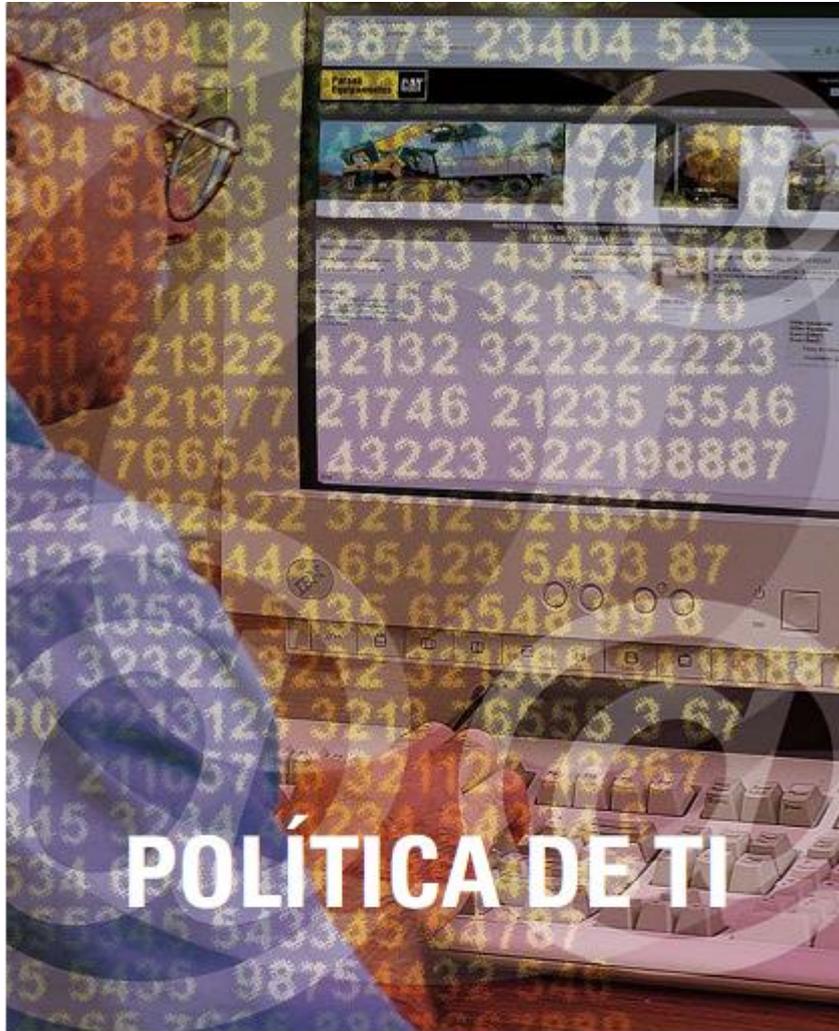
TI / Aqui Supermercados

Pág. 14

3. PROCEDIMENTOS

PROCEDIMENTOS AGENDADOS – SERVIDORES			
DESFRAGMENTAÇÃO DE DISCO			
SERVIDOR	HORÁRIO	UNIDADES	FREQUÊNCIA
Servidor03	4h	C:	Diária
Servidor03	5h	D:	Diária
Servidor01	15h	C:	Semanal / Domingo
Servidor01	12h	D:	Semanal / Domingo
Cpd1	15h	C:	Semanal / Domingo
Cpd1	12h	D:	Semanal / Domingo
DATA DA ÚLTIMA ALTERAÇÃO:			
15/01/2009 08:16			

ANEXO C



SUMÁRIO

1. INTRODUÇÃO	5
2. PROPÓSITO	6
3. ABRANGÊNCIA	6
4. DIREITOS DE USO	7
5. DEVERES CORRESPONDENTES	8
6. PROIBIÇÕES	10
7. COMPROMISSOS	12
8. SOFTWARES E LICENÇAS	14
9. ADIÇÃO E REMOÇÃO DE RECURSOS	14
10. ADMINISTRADOR DA REDE	15
11. AUDITORIA	15
12. USO DE SENHA	16



1 INTRODUÇÃO

A intenção da CSI (Comissão de Segurança da Informação) com a publicação da Política de Uso Aceitável, não é impor restrições contrárias à cultura de abertura e confiança da Paraná Equipamentos S.A, mas proteger a Empresa, nossos funcionários e parceiros, de ações ilegais ou danosas praticadas por qualquer indivíduo, de forma proposital ou inadvertidamente.

Sistemas relacionados à Internet/Intranet/Extranet - incluídos, mas não limitados, os equipamentos de computação, software, sistemas operacionais, dispositivos de armazenamento, contas de rede que permitem acesso ao correio eletrônico, consultas WWW e FTP a partir de IP's (endereços de protocolo da internet) e o sistema de telefonia - são propriedades da Paraná Equipamentos S.A., devendo ser utilizados com o exclusivo propósito de servir aos interesses da Empresa e de seus clientes, no desempenho de suas atividades empresariais.

A segurança efetiva é um trabalho de equipe envolvendo a participação e colaboração de todos os funcionários e afiliados de nossa Empresa que manipulam informações e/ou sistemas de informações. É de responsabilidade de cada usuário de computador conhecer esta política e conduzir suas atividades de acordo com a mesma.

2 PROPÓSITO

O propósito desta política é delinear a utilização aceitável dos equipamentos de informática e de telefonia da Paraná Equipamentos S.A. Estas regras foram definidas para proteger os funcionários e a Empresa. A utilização inapropriada dos equipamentos e sistemas relacionados no item anterior torna-os vulneráveis à atuação de hackers, contaminação por “vírus” e danificação, gerando comprometimento dos sistemas e serviços da rede, além de problemas legais.

3 ABRANGÊNCIA

Esta política se aplica aos funcionários, prestadores de serviços, consultores, auditores, fiscais, temporários e demais colaboradores que estejam a serviço da Paraná Equipamentos S.A., incluindo toda a mão-de-obra terceirizada ou disponibilizada mediante convênios, parcerias ou quaisquer outras formas de atuação conjunta com outras empresas; e abrange todos os sistemas e equipamentos de propriedade da Paraná Equipamentos S.A., bem como aqueles de propriedade de terceiros que lhe sejam confiados a qualquer título, ou cedidos pela mesma a terceiros.

4 DIREITOS DE USO

Os colaboradores da Paraná Equipamentos têm os seguintes direitos:

- 4.1. Fazer uso legal dos recursos computacionais colocados à sua disposição, respeitadas as normas de utilização estabelecidas pela Empresa;
- 4.2. Ter conta de acesso à rede corporativa, respeitadas as normas de utilização estabelecidas pela Empresa;
- 4.3. Ter conta de correio eletrônico com a extensão do domínio da Empresa, vetado o acesso a e-mails pessoais;
- 4.4. Acessar a Intranet e a Internet, respeitando as políticas da Empresa;
- 4.5. Acessar as informações que forem franqueadas, relativas às áreas de armazenamento privado e compartilhado, respeitadas as normas de utilização e confidencialidade estabelecidas pela Empresa;
- 4.6. Solicitar suporte técnico sempre que verificado o mau funcionamento dos equipamentos ou do sistema de rede corporativa;
- 4.7. Fazer uso do telefone da Empresa para tratar de assuntos relacionados ao trabalho.

5 DEVERES CORRESPONDENTES

Os usuários da rede corporativa têm as seguintes obrigações:

- 5.1. Responder pelo uso exclusivo de sua conta pessoal de acesso à rede corporativa;
- 5.2. Identificar, classificar e enquadrar as informações da rede corporativa relacionadas às atividades por si desempenhadas;
- 5.3. Zelar por toda e qualquer informação armazenada na rede corporativa contra alteração, destruição, divulgação, cópia e acessos não autorizados;
- 5.4. Guardar sigilo das informações confidenciais, mantendo-as em caráter restrito;
- 5.5. Manter, em caráter confidencial e intransferível, a senha de acesso aos recursos computacionais e de informação da organização, informando-a formalmente ao Administrador da Rede;
- 5.6. Informar imediatamente à Gerência sobre quaisquer falhas ou desvios das regras estabelecidas neste documento, bem como sobre a ocorrência de qualquer violação às mesmas, praticada em atividades relacionadas ao trabalho, dentro ou fora das dependências da Empresa;

-
- 5.7. Responder cível e criminalmente pelos danos causados em decorrência da não observância das regras de proteção da informação e dos recursos computacionais da rede corporativa;
 - 5.8. Fazer uso dos recursos computacionais para trabalhos de interesse exclusivo da organização;
 - 5.9. Fazer a emissão de pedidos de compra de recursos computacionais e a confirmação do recebimento das compras à administração, via e-mail, com cópia ao gestor.

6 PROIBIÇÕES

É proibido aos usuários da rede:

- 6.1. Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais (copyright), bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista ou que faça apologia ao crime;
- 6.2. Utilizar os recursos computacionais ou quaisquer outros de propriedade da Empresa, colocados à disposição do colaborador em razão do exercício de sua função, para constranger, assediar, prejudicar ou ameaçar a mesma ou terceiros, sejam eles indivíduos ou organizações;
- 6.3. Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade da Empresa, colocados à disposição do colaborador em razão do exercício de sua função;
- 6.4. Alterar os sistemas padrões, sem autorização;
- 6.5. Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;
- 6.6. Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;

- 6.7. Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
- 6.8. Utilizar acesso discado através de modem, ou qualquer outra forma de conexão não autorizada, quando conectado às redes instaladas nas dependências da Empresa;
- 6.9. Acessar e-mail pessoal;
- 6.10. Fazer uso do telefone da Empresa para discussão de assuntos pessoais;
- 6.11. Utilizar quaisquer recursos ou equipamentos da Empresa para fins diversos daqueles necessários ao desempenho da função contratada;
- 6.12. Criar blogs e comunidades na Internet, ou qualquer ambiente virtual semelhante, utilizando-se, sem autorização expressa, da logomarca da Empresa;
- 6.13. Fazer uso do telefone celular particular dentro das dependências da Empresa.

7 COMPROMISSOS

Os usuários da rede comprometem-se a:

- 7.1. Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores;
- 7.2. Não desenvolver, fomentar ou promover ações que incentivem o racismo ou qualquer tipo de discriminação que viole quaisquer outros direitos constitucionais do cidadão;
- 7.3. Não fazer uso da rede para molestar, ameaçar ou ofender seus usuários ou terceiros, por quaisquer meios, sejam textos, imagens, vídeos ou correios eletrônicos;
- 7.4. Não fazer uso da rede para circulação de propaganda política;
- 7.5. Não tomar atitude ou ação que possa, direta ou indiretamente, indisponibilizar recursos da rede corporativa;
- 7.6. Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilização de serviços;
- 7.7. Não executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa da Empresa;

- 
- 7.8. Não utilizar nenhum programa de bate-papo ou de mensagem instantânea, tais como Skype, MSN e Google Talk, entre outros;
 - 7.9. Não enviar informações confidenciais (autorizadas) para e-mails externos sem proteção. No mínimo, o arquivo deve contar com a proteção de uma senha “robusta”;
 - 7.10. Responsabilizar-se perante a Empresa e terceiros por quaisquer prejuízos advindos da violação dos compromissos, deveres e proibições estabelecidas nesse documento;
 - 7.11. Utilizar-se, de forma ética e em conformidade com as normas de conduta e segurança estabelecidas pela Empresa, de todos os recursos, equipamentos e informações que lhe sejam confiados em razão do desempenho de sua atividade profissional.

8 SOFTWARES E LICENÇAS

- 8.1. Todo software executado nos equipamentos da rede corporativa da Paraná Equipamentos deverá ser licenciado, sendo vetada a utilização de qualquer software sem licença;
- 8.2. A utilização de softwares livres ou temporários deverá ser solicitada ao responsável pela administração da rede, por escrito e, em caso de aprovação, a instalação e remoção deverão ser realizadas pelo mesmo;
- 8.3. A utilização de softwares não licenciados é considerada uma Não-Conformidade Gravíssima e acarretará punições ao funcionário ou colaborador, em qualquer nível, da Paraná Equipamentos.

9 ADIÇÃO E REMOÇÃO DE RECURSOS

É vetada aos usuários da rede de computadores da organização a adição e remoção de quaisquer recursos, sejam eles microcomputadores, impressoras, pen-drives, mp3 players ou outros equipamentos e dispositivos. A adição e remoção desses deverão ser solicitadas ao setor responsável, para aprovação e, em caso positivo, tais procedimentos deverão ser realizados pelo mesmo.

10 ADMINISTRADOR DA REDE

- 10.1. O uso das senhas e informações dos usuários, pelo Administrador da Rede, deverá ser realizado com fins operacionais e preventivos, cabendo ao Administrador manter a confidencialidade das informações adquiridas, sob pena de punição;
- 10.2. O controle das senhas dos usuários da PESA, deve ser feito pelo Administrador da Rede, e reportado formalmente para a Alta Direção da Empresa com as devidas atualizações.

11 AUDITORIA

- 11.1. Todos os funcionários que utilizam a rede corporativa (informática e telefonia) serão submetidos à auditoria, realizada por um profissional da administração da rede Paraná Equipamentos ou empresa especializada, com o objetivo de verificar o cumprimento das normas estabelecidas;
- 11.2. A auditoria ocorrerá semanalmente em microcomputadores ou notebooks escolhidos aleatoriamente e, caso verificada alguma não-conformidade, será instaurada uma sindicância interna voltada à apuração de responsabilidades e classificação da gravidade da violação das normas de utilização dos equipamentos;
- 11.3. Após a classificação da gravidade (alta, média ou baixa), a não-conformidade será comunicada ao Comitê de Ética para adoção das providências cabíveis.

12 USO DE SENHA

- 12.1. Cada usuário da rede corporativa da Paraná Equipamentos deverá informar formalmente ao Administrador da Rede suas senhas de acesso à máquina e ao servidor. Quando o Administrador da Rede solicitar a alteração das senhas, o usuário deverá fazê-lo e proceder à nova comunicação ao mesmo;
- 12.2. A responsabilidade pela manutenção do sigilo das senhas é exclusiva do colaborador, ao qual é proibido divulgar as senhas pessoais de acesso à rede corporativa a terceiros, exceto na hipótese descrita no item 10.



POLÍTICA DE TI

O colaborador abaixo nominado declara, para os fins de Direito, livre de qualquer impedimento, que por serem de propriedade da empresa, todos os equipamentos, sistemas, acessos à rede corporativa e e-mails corporativos, bem como os terminais de telefonia fixa ou móvel, somente poderão ser utilizados para o desempenho das funções profissionais, e nos seus limites, conforme a legislação pertinente e normas internas, no interesse da Paraná Equipamentos S.A..

Assim sendo, o colaborador abaixo nominado reconhece a legitimidade da Paraná Equipamentos S.A. para monitorar suas atividades laborativas, com a finalidade de manutenção da ordem e segurança pessoal de seus colaboradores, bem como da integridade da rede corporativa (informática e telefonia) e dos equipamentos e sistemas de sua propriedade, além do necessário sigilo das informações.

Pelos mesmos motivos, o colaborador abaixo nominado declara ter recebido, lido e concordado com todas as normas estabelecidas neste documento, autorizando, por este ato, a empresa, a monitorar qualquer atividade computacional e de telefonia realizada, em especial os e-mails e as ligações telefônicas geradas ou recebidas através dos terminais telefônicos da empresa, além de inventariar periodicamente o histórico de e-mails, ligações efetuadas, recebidas e outros itens correlacionados.

Eu, _____, declaro estar ciente dos termos das políticas de segurança relacionadas neste documento e autorizo o monitoramento de minhas atividades computacionais e de telefonia pela Paraná Equipamentos S.A., estando ciente dos meus direitos, obrigações e deveres para com esta empresa.

_____, _____ de _____ de _____

Assinatura

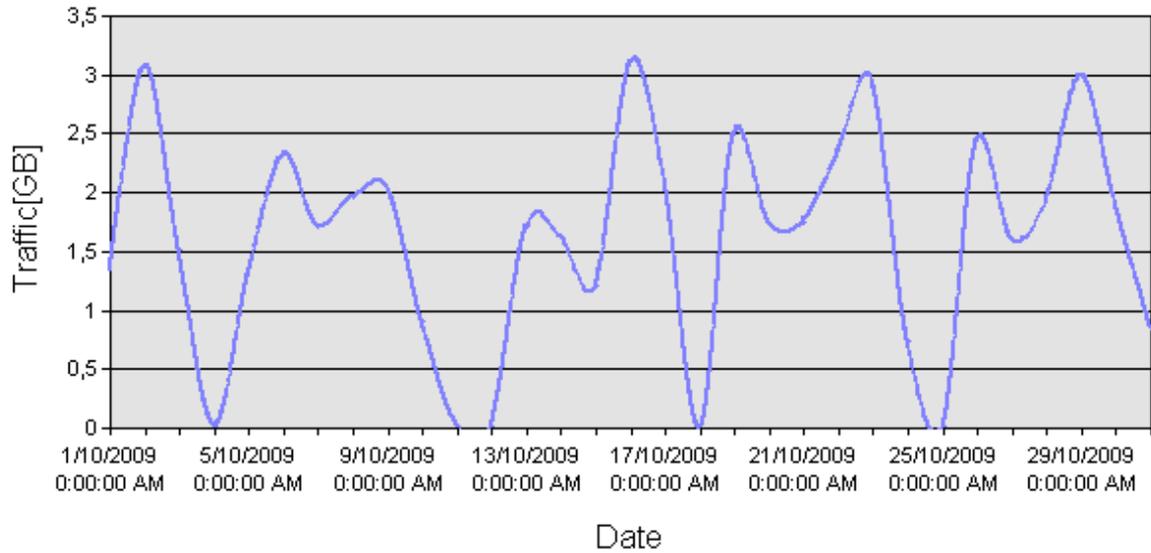
CPF: _____

ANEXO D

ISA SERVER 2006 REPORT

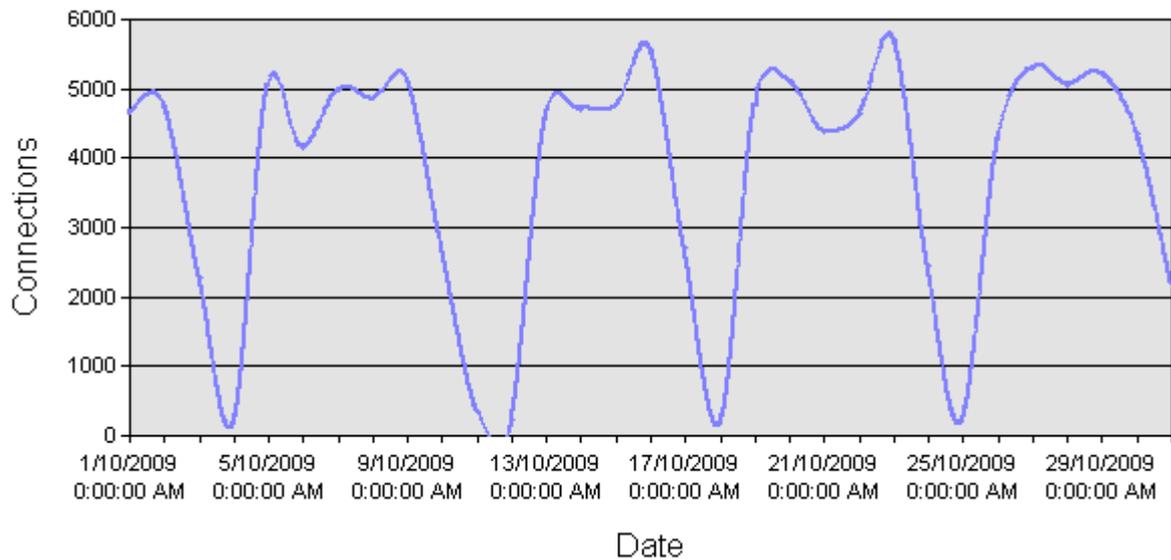
Traffic

The following chart summarizes the amount of network traffic, by date, sent through ISA Server. This report includes both Web and non-Web traffic.



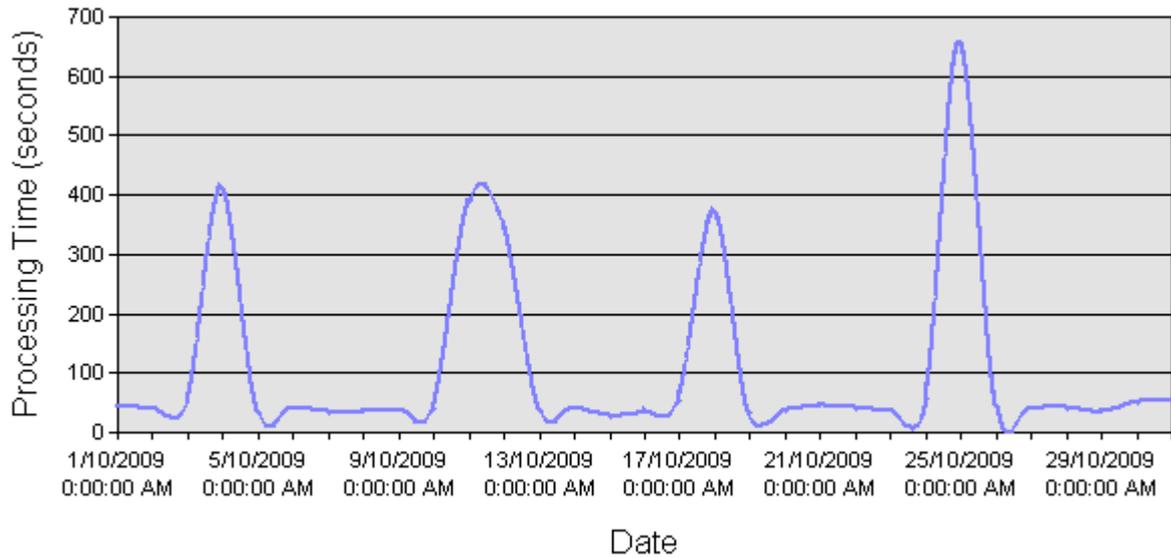
Connections

The following chart summarizes the peak number of simultaneous connections during each day of the report period.



Processing Time

The following chart summarizes the average request processing time during each day of the report period.



Daily traffic

The following chart summarizes average network traffic through ISA Server at various times during the day. This report includes both Web and non-Web traffic.

