VERIS EDUCACIONAL

FACULDADE DE TECNOLOGIA IBTA

PÓS-GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO

EDUARDO MARTINS PEREIRA
FERNANDO BRACALENTE
MARCELO DINOFRE
MARIO LUIZ BERNARDINELLI

PLANO DE SEGURANÇA DA INFORMAÇÃO
M2FE MÁQUINAS LTDA

CAMPINAS
2009

Eduardo Martins Pereira *(eduardomartinsp@gmail.com, eduardomp@globo.com)*
Fernando Bracalente (*bracalente@hotmail.com*)
Marcelo Dinofre (*mdinofre@hotmail.com*)
Mario Luiz Bernardinelli (*mariolb@gmail.com, mariolb@mariolb.com.br*)

Plano de Segurança da Informação M2FE Máquinas Ltda

Trabalho de conclusão de curso apresentado como parte das atividades para obtenção do título de especialista, do curso de Segurança da Informação da Faculdade de Tecnologia IBTA.

Orientador: Prof. MSc. Nelson Uto

CAMPINAS
2009

Autoria: Eduardo Martins Pereira
Fernando Bracalente
Marcelo Dinofre
Mario Luiz Bernardinelli

Título: Plano de Segurança da Informação - M2FE Máquinas Ltda

Trabalho de conclusão de curso apresentado como parte das atividades para obtenção do título de especialista, do curso de Segurança da Informação da Faculdade de Tecnologia IBTA.

Os componentes da banca de avaliação, abaixo listados, consideram este trabalho aprovado.				
	Nome	Titulação	Assinatura	Instituição
1	Nelson Uto	MSc		IBTA
2	Edmar Rezende	MSc		PUC Campinas
3	Fernando Amatte	Esp.		IBTA

Data da aprovação: 24 de Outubro de 2009.

Ao meu pai Carlos (in-memoriam) e minha mãe Virginia que me criaram e orientaram para o caminho da retidão. A minha esposa Maria Aparecida (Cida) e meus filhos Carolina (Carol) e Raphael (Rapha) que sempre me apoiaram e souberam entender as minhas longas ausências dedicadas a mais um estudo.

Eduardo Martins Pereira

Ao meu pai Orlando Bracalente e minha mãe Maria José Marcolin Bracalente pelo esforço em oferecer a melhor educação possível ante as dificuldades da vida. À minha esposa Graziela pelo apoio incondicional em todos os meus projetos.

Fernando Bracalente

Aos meus pais, pela minha criação e formação pessoal. Aos meus avós paternos (in-memoriam), símbolos de garra e luta dedicados ao trabalho pesado, durante suas vidas. Aos meus avós maternos, que sempre me apoiaram nos estudos. A minha namorada Adriana Galvão por fazer parte da minha vida.

Marcelo Dinofre

Ao meu pai Mario (in-memoriam) e minha mãe Roza pelo esforço em oferecer a melhor educação possível ante as dificuldades da vida. À minha esposa Elizete e ao meu filho Pedro Francisco pelo apoio incondicional em todos os meus projetos.

Mario Luiz Bernardinelli

AGRADECIMENTOS

Ao Grande Arquiteto do Universo, que me permitiu chegar aos 50 anos com muita saúde, sabedoria e determinação para galgar mais esse degrau na escada da vida. Aos meus amigos que fortaleceram os laços de igualdade e fraternidade. A minha família pelo apoio e compreensão. Ao meu professor e orientador MSc. Nelson Uto pela dedicação, determinação e comprometimento com o resultado deste trabalho.

Eduardo Martins Pereira

Aos meus pais pela formação e pelos sacrifícios feitos durante a criação dos filhos. A minha esposa Graziela T. P. Bracalente, pela paciência e incentivo nos momentos de desânimo. Ao término deste trabalho, quero expressar o meu agradecimento a todas as pessoas que, direta ou indiretamente colaboraram para sua concretização e ao professor MSc. Nelson Uto pela orientação dada ao nosso trabalho de conclusão de curso.

Fernando Bracalente

AGRADECIMENTOS

A Deus, pela minha vida e por ter me concebido saúde e sabedoria para conclusão de mais este curso. Aos colegas Eduardo, Fernando e Mario, pela dedicação e comprometimento, para realização deste trabalho. Ao Mestre Prof. Nelson Uto, pela orientação e dedicação prestada na realização deste trabalho. A minha namorada Adriana Galvão, pela paciência nos momentos de ausência e pelo apoio constante para realização deste trabalho. A todos em geral que contribuíram para minha formação pessoal e profissional.

Marcelo Dinofre

A Deus, por mais esta oportunidade. À minha esposa Elizete e meu filho Pedro Francisco, pelo apoio incondicional e compreensão pelos momentos de minha ausência. Ao meu amigo e ex-diretor José Orlando Gomes de Castro (in memorian), pelo apoio e auxílio nas traduções de textos, mas que nos deixou antes de ver o resultado final deste trabalho. Ao professor MSc. Nelson, Uto pela amizade, dedicação, auxílio e atenção prestados durante esta jornada. Aos colegas da turma SEG-15 pelos momentos de alegria, companheirismo e auxílio durante o curso.

Mario Luiz Bernardinelli

“O uso da palavra hacker para se referir ao violador de segurança é uma conclusão que vem por parte dos meios de comunicação de massa. Nós, hackers, nos recusamos a reconhecer este significado e continuamos usando a palavra para indicar alguém que ama programar e que gosta de ser hábil e engenhoso.”

Richard Stallman

RESUMO

Este trabalho de conclusão de curso apresenta como a segurança da informação muitas vezes é negligenciada pelas organizações até a ocorrência de incidentes graves, quando então são tomadas medidas para evitá-los. Apresenta as dificuldades em manter seguras as informações e demonstra que a segurança da informação é um processo cíclico, que deve ser mantido e atualizado permanentemente. Apresentamos o cenário de uma empresa envolvida num desses incidentes e que teve informações confidenciais do projeto de um novo produto descobertos no equipamento de um funcionário e que possivelmente foram enviadas para um concorrente. Este incidente provocou prejuízos financeiros diretos, o comprometimento de vendas futuras e a imagem da empresa. Diante de tal situação e da sensação de fragilidade, a empresa contratou os serviços de um CSO que definiu uma metodologia de análise de riscos, identificou os principais processos da empresa e os ativos envolvidos, realizou a análise de riscos inicial e apresentou para a presidência as vulnerabilidades, o impacto para o negócio e os custos envolvidos na sua mitigação e/ou controle. Concomitantemente à análise de riscos inicial iniciou-se o processo de criação das políticas de segurança da informação, procedimentos, plano de continuidade dos negócios, treinamento de colaboradores e o plano de gestão da segurança. Após aprovação pela presidência, diversos controles foram implementados, e uma nova análise de riscos realizada. As informações foram disponibilizadas para os executivos compararem os resultados e a evolução do serviço realizado.

Palavras-chaves: segurança da informação, análise de riscos, vulnerabilidades, plano de continuidade de negócios, gestão da segurança da informação.

ABSTRACT

The present work examines how information security is often neglected by the organizations up to the incidence of a serious event, upon which immediate measures-actions are taken to prevent it from happening again. It shows the difficulties faced up to keep the information safe and demonstrates the cyclic nature of the activities related to information security that must be continuously maintained and updated. A scenario is presented where a company is involved in one of these incidents when confidential information related to the design of a new product was disclosed to a competitor, causing direct financial loss, future sales uncertainty and company image damage.

A CSO specialist was hired to define a metodology of risk analysis, map the main internal processes and the involved assets, develop the initial risk analysis, prepare a report to point out the vulnerabilities, impact on the business and costs to mitigate and/or control all risks. Simultaneously to the initial risk analysis a number of other related activities was started to create information security policies, procedures, business continuity plan, training of associates and security management plan. After the approval of the company's presidency, many controls were implemented and a new risk analysis was performed. Final results were made available for the high (staff-management) to evaluate the achievements of the service just provided.

Keywords*: information security, risk analysis, vulnerabilities, business continuity plan, information security management.*

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

SUMÁRIO

INTRODUÇÃO

Atualmente, a segurança da informação é um assunto de crescente destaque e preocupação nas empresas principalmente após o advento da Internet e da digitalização das informações.

Cada vez mais as empresas se veem alvos de ataques que visam obter as informações essenciais e mais valiosas da empresa. Estes ataques podem ocorrer das mais variadas formas e podem ser de origem interna ou externa.

Este trabalho tem por objetivo demonstrar os passos executados para tornar a informação da empresa mais segura, levando-se em conta os riscos existente atualmente. Ele parte de uma situação onde a empresa foi vítima de um vazamento de informação que expôs um projeto confidencial, apresenta o levantamento da situação atual e as ações necessárias para melhorar a segurança.

A apresentação dos fatos e ações procura seguir a ordem cronológica dos seus acontecimentos, sendo que algumas atividades ocorrem em paralelo com outras. A ordem correta é apresentada no cronograma das atividades na Figura 21.

Este trabalho foi desenvolvido com a participação das seguintes pessoas:

- Eduardo Martins Pereira
- Fernando Bracalente
- Marcelo Dinofre
- Mario Luiz Bernardinelli

1 APRESENTAÇÃO DA EMPRESA

Em 1997, um grupo de quatro amigos concluiu que havia uma boa oportunidade de negócio na área de embalagens para a indústria química. Desta oportunidade nasceu uma sociedade que se transformou na M2FE Máquinas Ltda.

Localizada em Campinas, estado de São Paulo, a M2FE sempre procurou utilizar as mais modernas tecnologias existentes no mercado, além de desenvolver as suas próprias soluções.

Graças à qualidade de seus produtos e assistência técnica, a M2FE teve um rápido crescimento.

Atualmente, pouco mais de dez anos desde a sua criação, a M2FE conta com uma unidade fabril e dois escritórios estratégicos, um em Curitiba e outro no Rio de Janeiro. Toda esta estrutura é mantida em operação com aproximadamente 70 colaboradores e promove um faturamento médio anual de 14 milhões de reais.

Sempre em expansão, mas sem perder o foco, a M2FE tem como missão produzir máquinas envasadoras, enchedoras e manipuladoras para a indústria química, atender às necessidades de seus clientes, oferecer soluções completas, ser referência no mercado de máquinas, investir em tecnologia de ponta e atualizar seus colaboradores.

2 A SEGURANÇA DA INFORMAÇÃO

Quando iniciamos a construção de uma casa, começamos com um projeto que conta com duas partes básicas: a primeira e mais bonita, nos dá uma ideia bem clara de como ela será (arquitetura). Já a segunda descreve como deverá ser a sua estrutura a fim de suportar o peso da casa, além de especificar onde serão locados os pilares e como deverão ser as suas vigas. Então, começamos a construção pela fundação, que deve ser resistente o suficiente para suportar todo o resto e depois construímos a sua estrutura e paredes. Após são efetuados os acabamentos, conforme descrito no projeto.

Durante todo o processo de construção, os engenheiros acompanham a obra para garantir que as especificações do projeto estão sendo seguidas. Terminada a construção, ela é inspecionada para garantir que pode ser habitada com segurança.

Observe que a construção de uma casa requer todo um cuidado especial: tudo deve ser planejado e o projeto deve ser seguido durante todo o processo de construção. Sem um projeto, poderiam ocorrer muitos erros, como portas e janelas alocadas erroneamente. Pior ainda, a estrutura da casa poderia não suportar a carga imposta pela construção e poderiam surgir rachaduras, não passaria pela inspeção e, consequentemente, não poderia ser habitada. Uma condição destas representa uma perda enorme de tempo e de investimento.

Um programa de segurança em alguns aspectos básicos, é muito parecido com o processo de construção de uma casa: é preciso planejamento, execução e controle durante toda a sua construção. Para que um programa de segurança em uma instituição funcione, é preciso um estudo das reais necessidades da mesma, com foco na missão da instituição. Depois, é necessário um levantamento das condições atuais dos processos existentes e dos principais serviços utilizados.

Finalizada a etapa de levantamento, devem ser avaliadas todas as possíveis ameaças que possam comprometer a realização da missão da instituição e as vulnerabilidades devem ser detectadas. De posse das vulnerabilidades levantadas, deve-se determinar os custos envolvidos e a prioridade de tratamento das mesmas. A partir de todas estas informações, deve-se partir para o processo de execução dos controles.

Devemos atentar para o fato de que cada etapa de um programa de segurança deve ser muito bem estudada e planejada, pois ela fornece insumos para as etapas subsequentes. Na área de segurança da informação, atividades pontuais podem não trazer o resultado esperado. Por exemplo, engana-se quem acha que a instalação e configuração de um *firewall* irá proteger a instituição contra ataques cibernéticos. Sem dúvida, o *firewall* tem uma função muito importante, mas ele é apenas uma parte da segurança. De nada adianta um *firewall* impenetrável, se a aplicação *Web* não tiver sido projetada com foco também em segurança.

Além disso, os processos são dinâmicos e sofrem alterações constantemente de acordo com as necessidades da instituição e do mercado. Da mesma forma, para acompanhar a evolução da instituição e de seus processos, os *softwares* também sofrem alterações. Neste cenário é imprescindível que a segurança seja repensada. Por exemplo, há alguns anos atrás, as redes sem fio não eram utilizadas intensamente nas empresas. Hoje elas são uma realidade e com ela surgiram novas ameaças às instituições, obrigando os setores de segurança a se adequarem a essa nova situação.

Com essas considerações queremos firmar o conceito de que o processo de segurança não tem fim: ele é cíclico. Com isto em mente, é imprescindível que a instituição tenha uma área que foque especificamente a segurança, e deve trabalhar em parceria com as demais áreas a fim de prover e garantir a segurança para os seus processos e ativos.

3 CONTEXTUALIZAÇÃO DA CONTRATAÇÃO DO *SECURITY OFFICER*

Sendo a M2FE uma empresa com visão de futuro, ela entende que a segurança é objeto de relevante importância para o cumprimento da sua missão. Para que este objetivo possa ser alcançado, é preciso que o seu ambiente esteja devidamente protegido, trazendo mais segurança para seus clientes, garantindo que dados e informações vitais e sigilosos estejam sempre íntegros e disponíveis apenas para os interessados, independente de onde sejam acessados. Para a M2FE, é de suma importância passar essa imagem para os seus clientes.

3.1 Motivação para a contratação do Security Officer

A M2FE sempre teve uma preocupação muito grande com a segurança de seus bens e funcionários. No entanto, a evolução tecnológica ocorrida nos últimos tempos fez com que a necessidade de segurança ultrapassasse o sentimento de proteger bens físicos: hoje a informação é um bem vital para a sobrevivência da corporação e deve ser devidamente protegida. Assim, ao mesmo tempo em que a informação deve ser praticamente onipresente, também deve estar disponível em qualquer momento e somente a pessoas devidamente autorizadas.

Um incidente ocorrido na M2FE serviu de alerta para a necessidade de cuidados especiais com as informações da empresa.

Em abril de 2008, um funcionário da M2FE, com acesso aos servidores das áreas de engenharia, PCP e também ao sistema ERP, copiou arquivos do projeto de uma nova máquina para seu computador.

Este fato foi descoberto ocasionalmente durante uma operação de suporte técnico em sua estação de trabalho quando o analista de suporte observou a existência desses arquivos. Este fato só chamou a atenção do analista de suporte pelo fato de que, em operações normais, os usuários dos arquivos de projetos não fazem cópias para seus computadores, mas somente os acessam pela rede a fim de garantir que sempre estão utilizando a versão atualizada. Outro fato relevante é que, junto com os arquivos de projeto encontrados no disco do computador, havia também arquivos de relatórios contendo a relação de clientes e o nome das pessoas chaves de contato.

Os arquivos encontrados eram da máquina mais moderna já produzida pela empresa, usando alta tecnologia embarcada e de grande valor agregado. Essa máquina representa um grande diferencial competitivo da M2FE em relação aos seus concorrentes e o projeto dela levou dois anos para ser concebido e viabilizado.

Como grande parte dos arquivos de desenhos, o projeto elétrico e o plano de montagem da nova máquina estavam nos arquivos encontrados no computador do usuário, estima-se um prejuízo direto de mais de dois milhões de reais, além do prejuízo incalculável com o comprometimento de vendas futuras e da própria imagem da empresa, pois meses depois do incidente, um concorrente lançou no mercado uma máquina similar à do projeto da M2FE.

Depois desta ocorrência, a Presidência da M2FE decidiu contratar os serviços de um CSO (*Chief Security Officer*) para que fossem avaliadas as reais condições do ambiente da empresa e para que as devidas providências fossem tomadas para evitar que incidentes deste tipo voltassem a ocorrer. A contratação do CSO ocorreu no dia 15 de Junho de 2008 e criou uma nova posição no organograma da empresa, na qual o CSO responde diretamente para a presidência, conforme organograma apresentado na Figura 1.

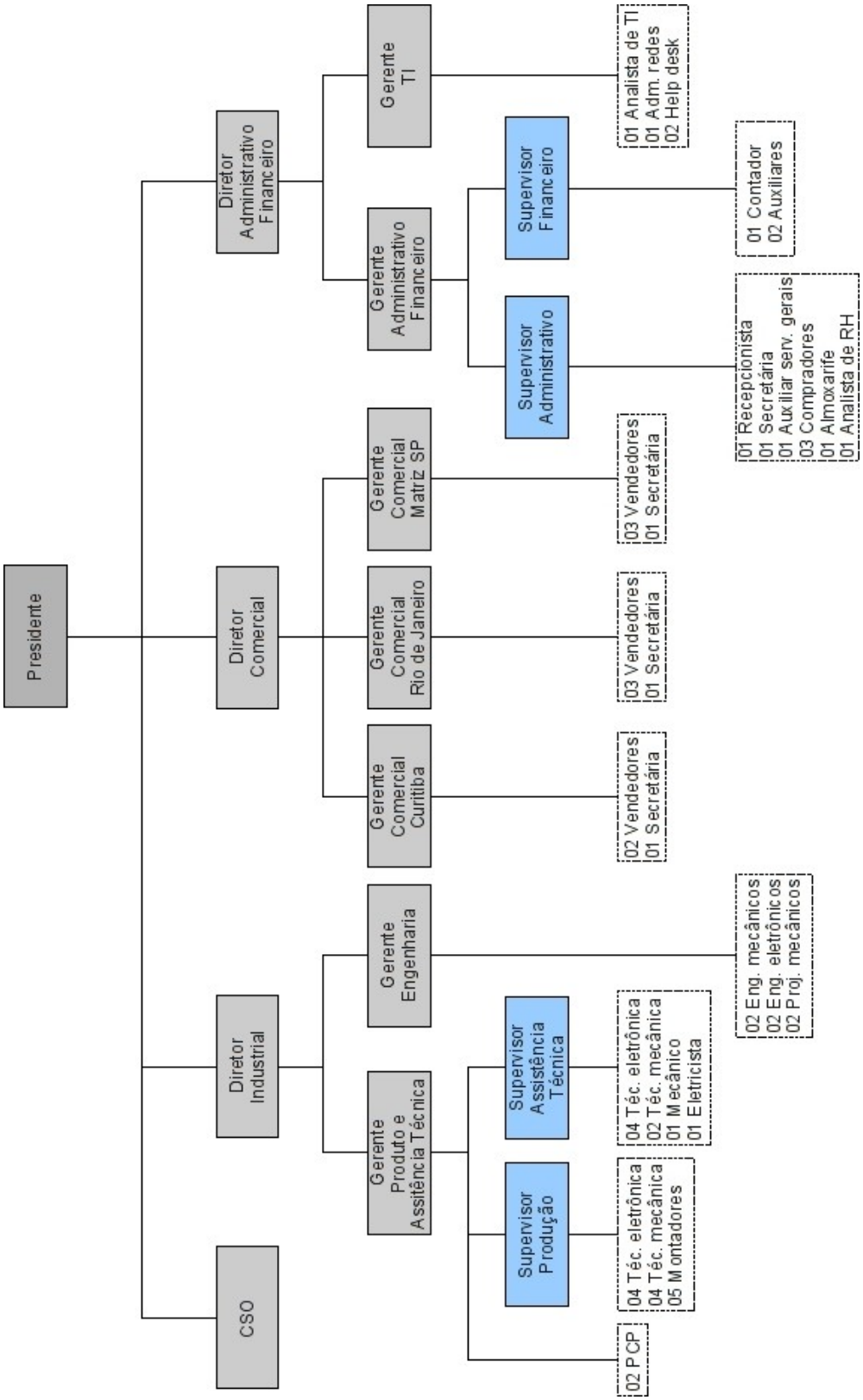


Figura 1: Organograma da M2FE

4 DESCRIÇÃO DA EMPRESA

4.1 Infraestrutura Física

4.1.1 Matriz

A planta baixa da matriz da M2FE pode ser observada na Figura 2.

A empresa M2FE está localizada em Campinas, estado de São Paulo, numa área plana e alta, não sendo portanto alvo de enchentes.

A planta baixa nos dá uma visão geral da implantação dos prédios da fábrica e do escritório. Pode ser observado que a empresa localiza-se em uma avenida.

Na parte frontal do terreno da empresa, há um estacionamento, que é separado das instalações da empresa por uma grade. Apesar de não estar representado na Figura 2, o terreno da M2FE faz divisa nas laterais e nos fundos com áreas ocupadas por outras empresas.

Para a monitoração da área externa da empresa, há três câmeras de CFTV móveis (giratórias), uma com visada para a área da portaria e duas outras instaladas no prédio do setor 2 da fábrica, com visada para a área entre os prédios da empresa. Estas câmeras estão conectadas a um sistema de gravação de imagens em DVR com retenção de imagens por trinta dias.

O acesso à empresa se faz através de uma portaria, onde o visitante é identificado e encaminhado para uma pequena sala junto à portaria para a confecção do crachá de visitante. Depois de identificado, o visitante é acompanhado por um funcionário até a recepção executiva, que fica na entrada do prédio principal, como pode ser observado com maiores detalhes na Figura 3.

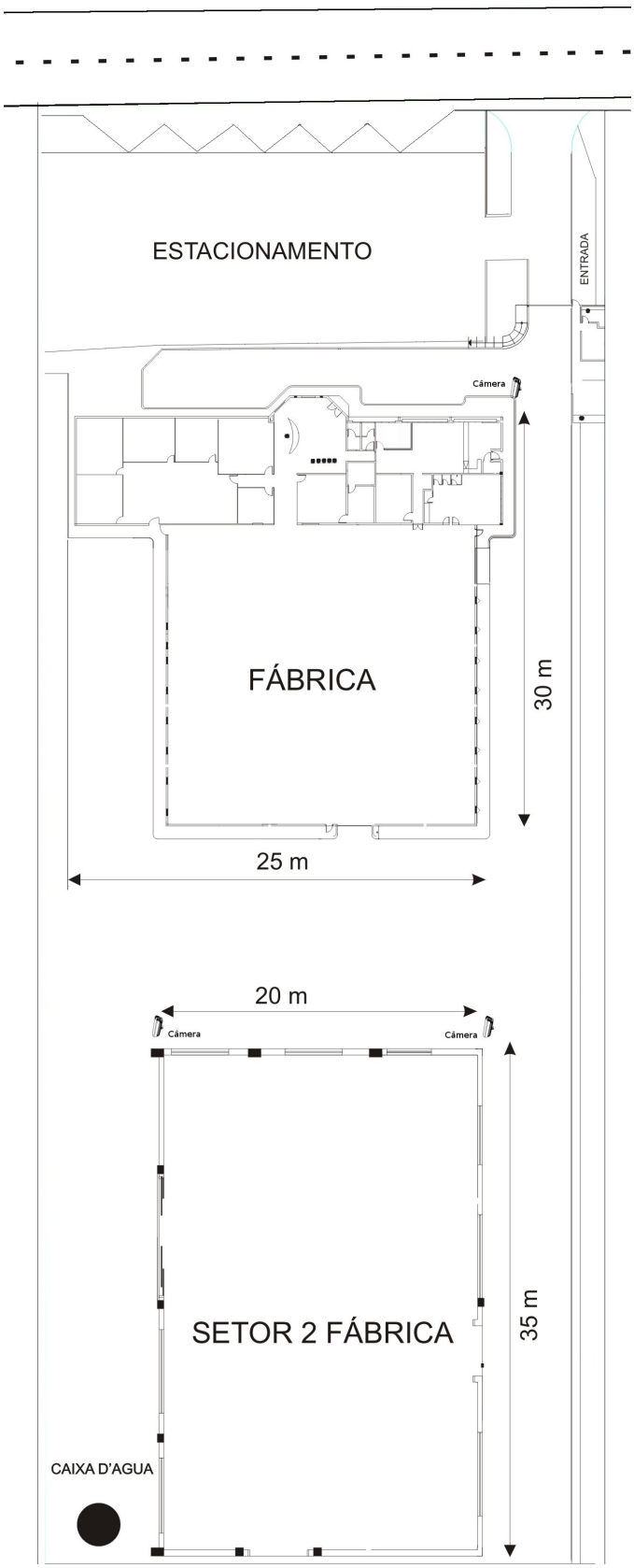


Figura 2: Planta baixa da Matriz

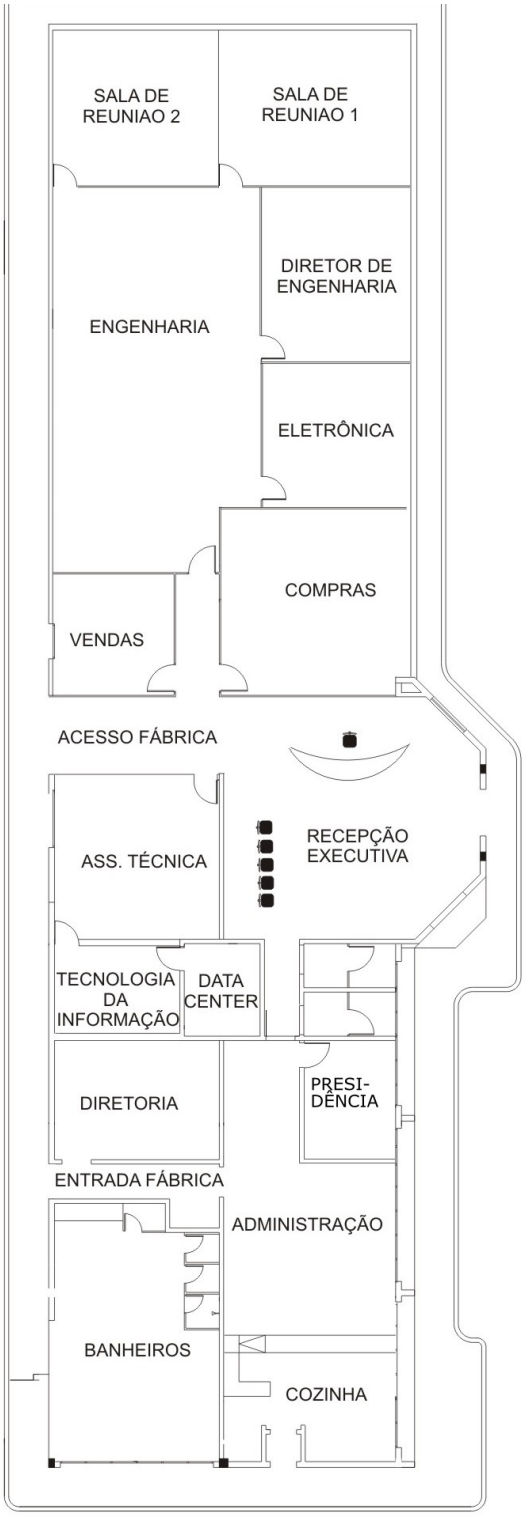


Figura 3: Planta baixa do prédio principal da matriz

4.1.2 Escritório de Curitiba

O escritório de Curitiba consiste numa sala no quarto andar de um edifício empresarial situado nas proximidades do centro da cidade.

A planta baixa deste escritório é apresentada na Figura 4.

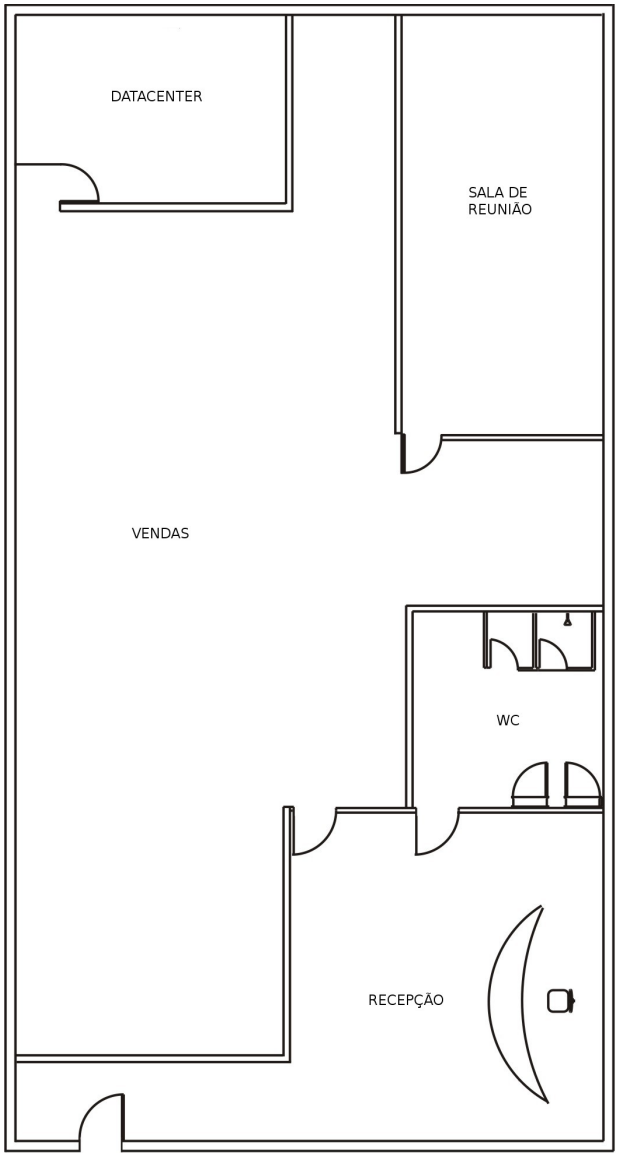


Figura 4: Planta baixa da filial Curitiba

A sala denominada *Data Center* é o local onde ficam atualmente o *switch,* o *link* dedicado com a matriz e o PABX.

4.1.3 Escritório do Rio de Janeiro

O escritório do Rio de Janeiro consiste numa sala no quinto andar de um edifício empresarial.

A planta baixa deste escritório é apresentada na Figura 5.

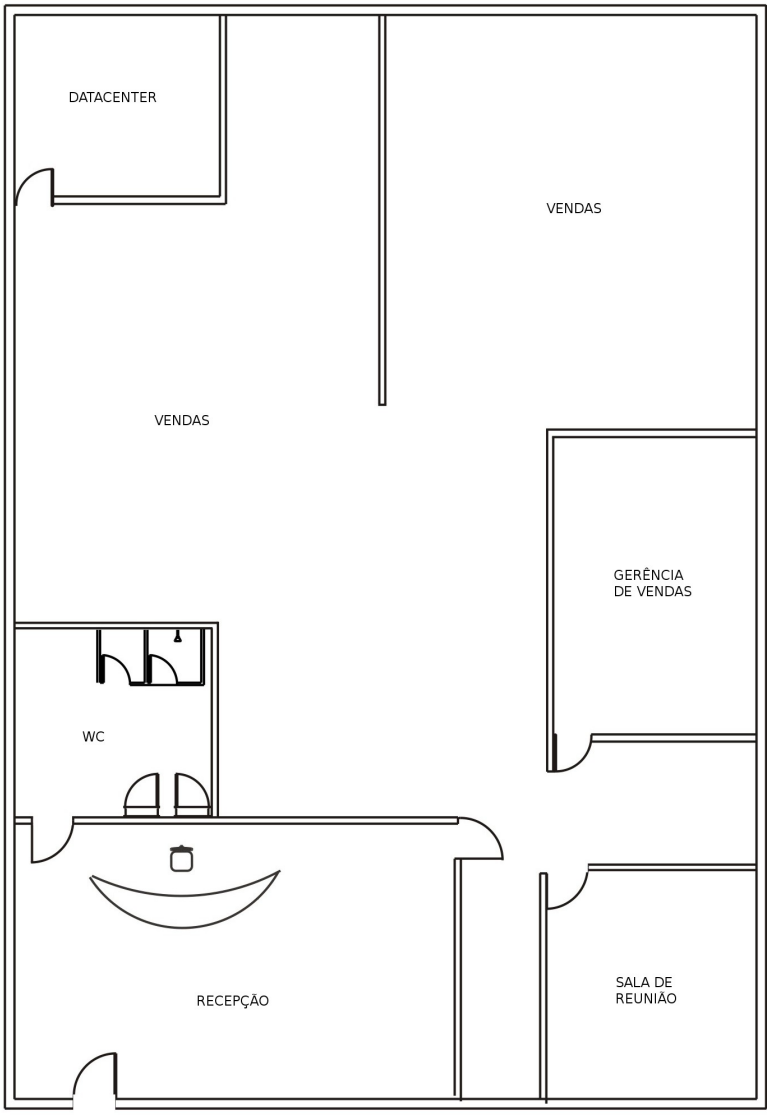


Figura 5: Planta baixa da filial Rio de Janeiro

A sala denominada *Data Center* é o local onde ficam atualmente o *switch,* o *link* dedicado com a matriz, o *link* ADSL e o PABX.

4.2 Infraestrutura Lógica

A Figura 6 ilustra a estrutura lógica da rede de computadores encontrada na M2FE.

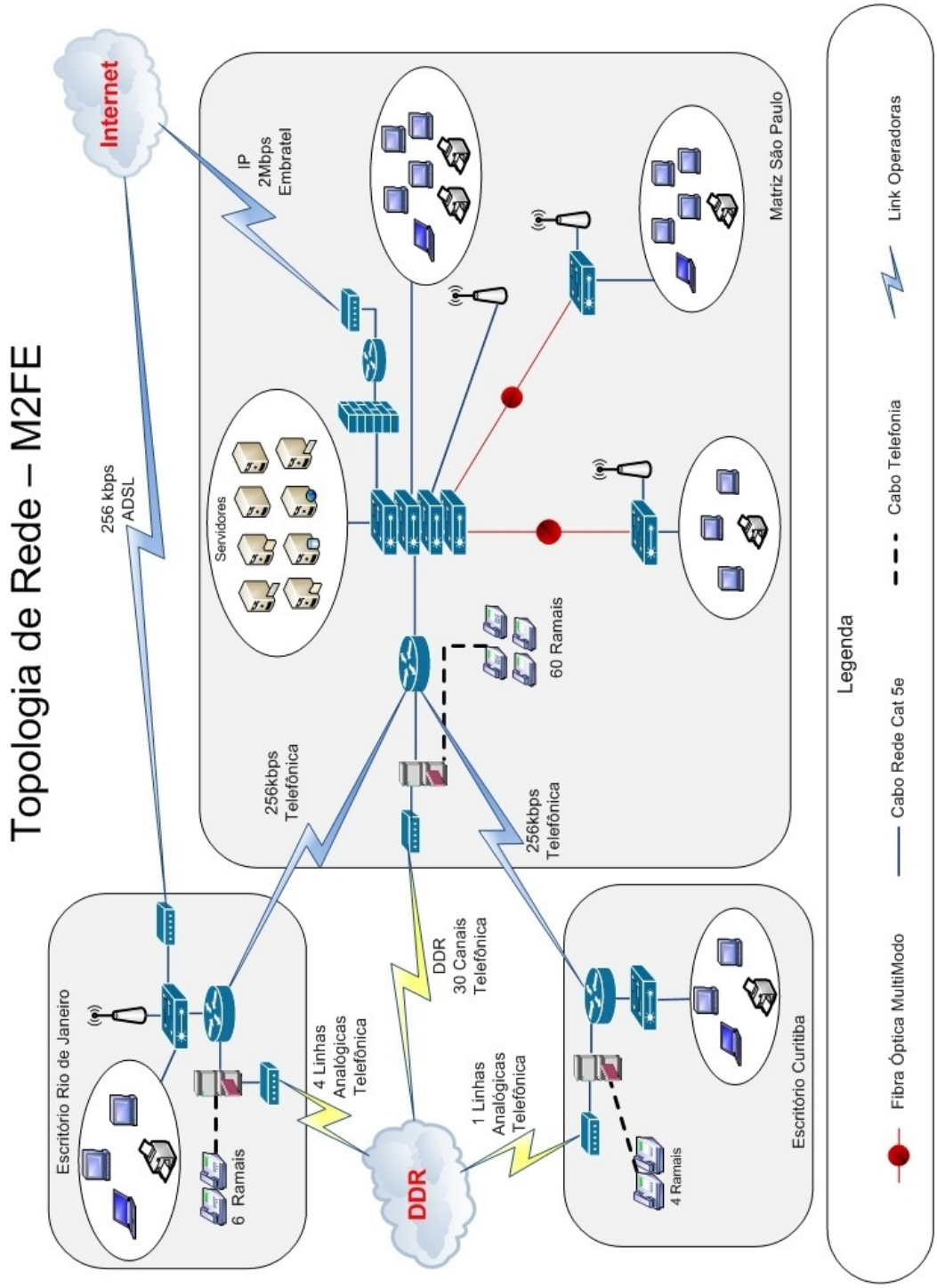


Figura 6: Estrutura lógica da rede da M2FE

A estrutura lógica atual da M2FE é composta por três partes: a estrutura principal localizada nas dependências da matriz e mais duas estruturas menores e mais simples localizadas nos escritórios de Curitiba e Rio de Janeiro.

Os principais ativos da infraestrutura da rede são:

- 1 Servidor de arquivos
- 1 Servidor *Web*
- 1 Servidor *Proxy*
- 1 Servidor de *e-mail*
- 1 Servidor do ERP
- 1 Servidor de banco de dados
- 1 Servidor *Active Directory* / DHCP / DNS
- 1 *Firewall*
- 1 Roteador de Internet

Estes servidores estão todos localizados na matriz e instalados no mesmo segmento de rede dos demais equipamentos, tais como as estações de trabalho, as impressoras de rede e, também, os três pontos de acesso à rede sem fio. A resolução interna de nomes é realizada pelo servidor *Active Directory* e para a resolução externa de nomes é utilizado o DNS do provedor de serviço de *Internet*.

A rede local da matriz conta com 56 estações de trabalho, 6 impressoras, 3 pontos de acesso à rede sem fio e diversos *notebooks*. A infraestrutura conta com um *link* de 2 Mbps para conexão com a Internet. Este acesso possui um *firewall* para prover a proteção da rede.

O sistema de telefonia conta com um PABX com suporte a VoIP e capacidade para 60 ramais. O *link* de comunicação com a rede de telefonia pública é um E1 (2Mbps). Tanto a matriz como os escritórios possuem PABX com suporte a VoIP. A conexão entre estes PABX se faz através do *link* de dados de 256 Kbps que interliga a matriz com os escritórios.

O escritório de Curitiba possui uma pequena rede local com 3 estações de trabalho, uma impressora, um ponto de acesso à rede sem fio e um *notebook*. Este escritório está interligado com a rede da matriz através de um *link* dedicado de 256 Kbps.

O escritório do Rio de Janeiro também possui uma estrutura simples, composta por 5 estações de trabalho, uma impressora, um *notebook* e um ponto de acesso à rede sem fio. O *link* com a matriz, também dedicado, é de 256 Kbps e há ainda com um *link* ADSL de 256 Kbps para acesso direto à *Internet*.

Com a finalidade de conhecer os equipamentos e sistemas operacionais das redes da empresa foi efetuado um levantamento das características básicas de cada unidade.

4.2.1 Mapeamento dos ativos da matriz

A lista de ativos e suas características básicas são apresentadas na Tabela 1 (Mapeamento dos ativos da matriz).

Tabela 1: Mapeamento dos ativos da matriz

Nome	***Endereço IP/Máscara***	***Tipo***	***Descrição***	***Local***	***Hardware***	***Software***
Roteador_sp_1	192.168.1.1/29	Rede	Roteador *Internet*	*Data center*	Cisco 1841	c1841-advsecurityk9-mz.124-3f.bin
PABX_sp_1	172.20.1.2/28	Rede	PABX HG Siemens VoIP	*Data center*	Siemens hipath	Versão 4
Roteador_sp_2	172.16.1.1/24	Rede	Roteador	*Data center*	Cisco 1751	c1751-ipbase-mz.123-3a.bin

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Firewall_sp_1	172.16.1.2/24	Rede	*Firewall* Linux *Netfilter*	*Data center*	HP Proliant DL 380 G3	GNU/ Linux Debian 4.0 (Etch)
Switch_sp_1	172.16.1.3/24	Rede	*Switch* dos servidores	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_2	172.16.1.4/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_3	172.16.1.5/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_4	172.16.1.6/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_5	172.16.1.7/24	Rede	*Switch* das estações de trabalho da fábrica	Rack_1	Cisco 2960	c2960-lanbase-mz.122-40.SE

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Switch_sp_6	172.16.1.8/24	Rede	*Switch* das estações de trabalho Almoxari-fado	Rack_2	Cisco 2960	c2960-lanbase-mz.122-40.SE
AP_sp_1	172.16.1.15/24	Rede	Rede sem fio	Rack_1	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
AP_sp_2	172.16.1.16/24	Rede	Rede sem fio	Rack_2	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
AP_sp_3	172.16.1.17/24	Rede	Rede sem fio	Rack_3	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
Domain_Server	172.16.1.20/24	Servidor	Active Directory	*Data center*	HP Proliant DL 380 G4	Windows 2003 SP2
Mail_Server	172.16.1.21/24	Servidor	Servidor de *e-mail*	*Data center*	HP Proliant DL 380 G4	Windows 2003 SP2 + Exchange 2003 SP2

Nome	***Endereço IP/Máscara***	***Tipo***	***Descrição***	***Local***	***Hardware***	***Software***
ERP_Server	172.16.1.22/24	Servidor	Servidor de aplicação	*Data center*	HP Proliant DL 380 G5	Windows 2003 SP1 + ERP
DB_Server	172.16.1.23/24	Servidor	Servidor de banco de dados	*Data center*	HP Proliant DL 380 G3	Windows 2003 SP2 + Oracle 9i
WEB_Server	172.16.1.24/24	Servidor	Servidor *Web*	*Data center*	HP Proliant DL 380 G3	Windows 2003 SP1
Proxy_Server	172.16.1.25/24	Servidor	*Proxy*	*Data center*	HP Proliant DL 380 G3	GNU/Linux Debian 4.0 (Etch) + Squid
MailGatetway_ Server	172.16.1.26/24	Servidor	*Anti Span*	*Data center*	HP Proliant DL 380 G3	GNU/Linux Debian 4.0 (Etch)
Printer_sp_01	172.16.1.40/24	Impressora	Impressora *laser* colorida	Diretoria	HP Color LasertJet 2840	-
Printer_sp_02	172.16.1.41/24	Impressora	Impressora *laser*	Diretoria	HP-P3005DN	-

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Printer_sp_03	172.16.1.42/24	Impressora	Impressora *laser*	Administrativo e Financeiro	HP-P3005DN	-
Printer_sp_04	172.16.1.43/24	Impressora	*Impressora laser*	Comercial	HP-P3005DN	-
Printer_sp_05	172.16.1.44/24	Impressora	*Laser Color Printer*	Comercial	HP Color LasertJet 2840	-
Printer_sp_06	172.16.1.45/24	Impressora	Impressora *laser*	Engenharia	HP-P3005DN	-
Printer_sp_07	172.16.1.46/24	Impressora	*Ploter*	Engenharia	HP Plotter 800	-
Printer_sp_08	172.16.1.47/24	Impressora	Impressora a jato de tinta	Montagem	HP Deskjet 630c	-
Printer_sp_09	172.16.1.48/24	Impressora	Impressora a jato de tinta	Almoxarifado	HP Deskjet 630c	-
Printer_sp_10	172.16.1.49/24	Impressora	Impressora Matricial	Faturamento	Epson DFX 8000	-
Printer_sp_11	172.16.1.50/24	Impressora	Impressora *laser*	TI	HP-P3005DN	-

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Printer_sp_12	172.16.1.51/24	Impressora	Impressora *laser*	Assist. Técnica	HP-P3005DN	-
DHCP	172.16.1.150/24 - 172.16.1.254/24	Estação de trabalho	Faixa de distribuição DHCP	-	-	-

4.2.2 Mapeamento dos ativos do escritório do Rio de Janeiro

Os ativos e suas características básicas do escritório do Rio de Janeiro podem ser observados na Tabela 2 (Mapeamento dos ativos do escritório do Rio de Janeiro).

Tabela 2: Mapeamento dos ativos do escritório do Rio de Janeiro

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Roteador_rj_1	192.168.2.1/30 a 172.17.1.1/24	Rede	*Modem* Roteador *Internet*	*Data center*	Dlink DSL-500 B	-
PABX_rj_1	172.20.2.2/28	Rede	HG Siemens VoIP	*Data center*	Siemens hipath	Versão 4
Roteador_rj_1	172.17.1.4/24	Rede	Roteador	*Data center*	Cisco 1751	c1751-ipbase-mz.123-3a.bin

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Switch_rj_1	172.17.1.2/24	Rede	*Switch* das estações de trabalho	Rack_1	Cisco 2960	c2960-lanbase-mz.122-35.SE
AP_rj_1	172.17.1.3/24	Rede	Rede sem fio	Rack_1	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
Printer_rj_01	172.17.1.40/24	Impressoras	Impressora *laser*	Diretoria	HP-P3005DN	-
DHCP	172.17.1.150/24 - 172.17.1.254/24	Estações de trabalho	Faixa de Distribuição DHCP	-	-	-

4.2.3 Mapeamento dos ativos do escritório de Curitiba

Os ativos e características básicas do escritório de Curitiba podem ser observados na Tabela 3 (Mapeamento dos ativos do escritório de Curitiba).

Tabela 3: Mapeamento dos ativos do escritório de Curitiba

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
PABX_pr_1	172.20.3.2/28	Rede	HG Siemens VoIP	*Data center*	Siemens hipath	Versão 4

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
Roteador_pr_1	172.17.2.1/24	Rede	Roteador	*Data center*	Cisco 1751	c1751-ipbase-mz.123-3a.bin
Switch_pr_1	172.17.2.2/24	Rede	*Switch* das estações de trabalho	Rack_1	Cisco 2960	c2960-lanbase-mz.122-35.SE
AP_pr_1	172.17.2.3/24	Rede	Rede sem fio	Rack_1	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
Printer_pr_01	172.17.2.40/24	Impressoras	Impressora *laser*	Diretoria	HP-P3005DN	-
DHCP	172.17.2.150/24 - 172.17.2.254/24	Estações de trabalho	Faixa de Distribuição DHCP	-	-	-

4.3 Processos

A partir do levantamento da topologia da rede, foi possível identificar os seus principais ativos. Para a realização da etapa de análise de riscos, precisamos mais do que simplesmente identificar os ativos de rede a serem protegidos: é preciso identificar os principais processos do negócio para estabelecermos a relação entre estes processos e os ativos de rede. Dessa forma, fica mais fácil a identificação dos ativos críticos para a execução da missão da empresa.

Para conhecer os processos de negócio da empresa, foram efetuadas pesquisas em campo, consultado os manuais de qualidade e efetuadas entrevistas com os executivos e gerentes da empresa.

Foram identificados os seguintes processos que regem a execução do negócio:

- Macro Processo de Vendas
    - Formalizar pedido
    - Aprovar protótipo
    - Controlar produção
    - Comprar componentes
    - Produzir produto
    - Faturar produto
- Macro Processo de Assistência Técnica
    - Atender cliente
    - Controlar produção de campo
    - Realizar serviços
    - Faturar serviços de campo
- Contábil, administrativo e financeiro

As figuras 7 a 20 apresentam a interação entre os processos e como eles se relacionam com as respectivas áreas. As partes em destaque significam que existe uma interação com os sistemas computacionais da M2FE.

Os processos contábil, administrativo e financeiro são executados como parte dos demais processos e, portanto, não são exibidos explicitamente nos diagramas.

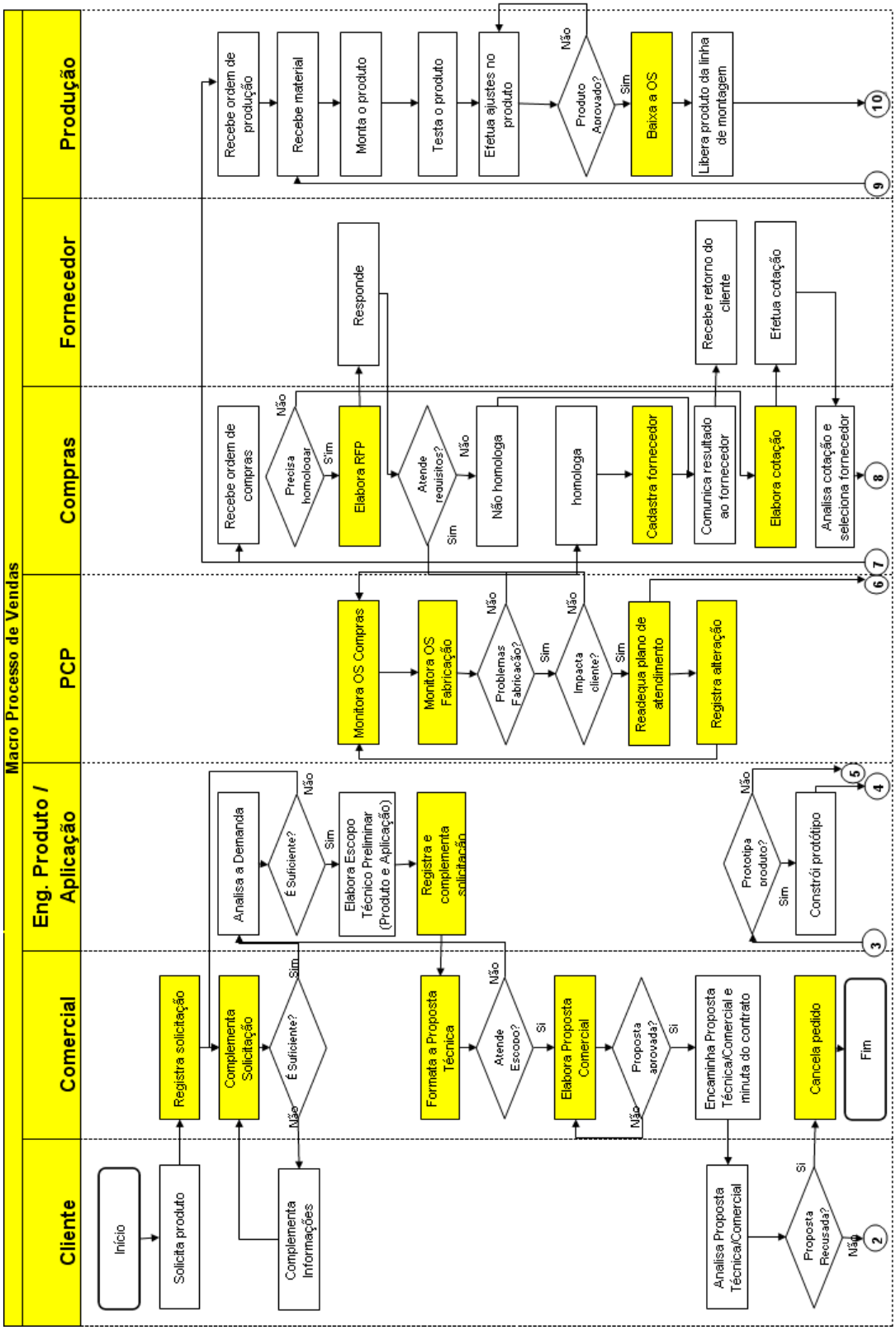


Figura 7: Macro processo de Vendas

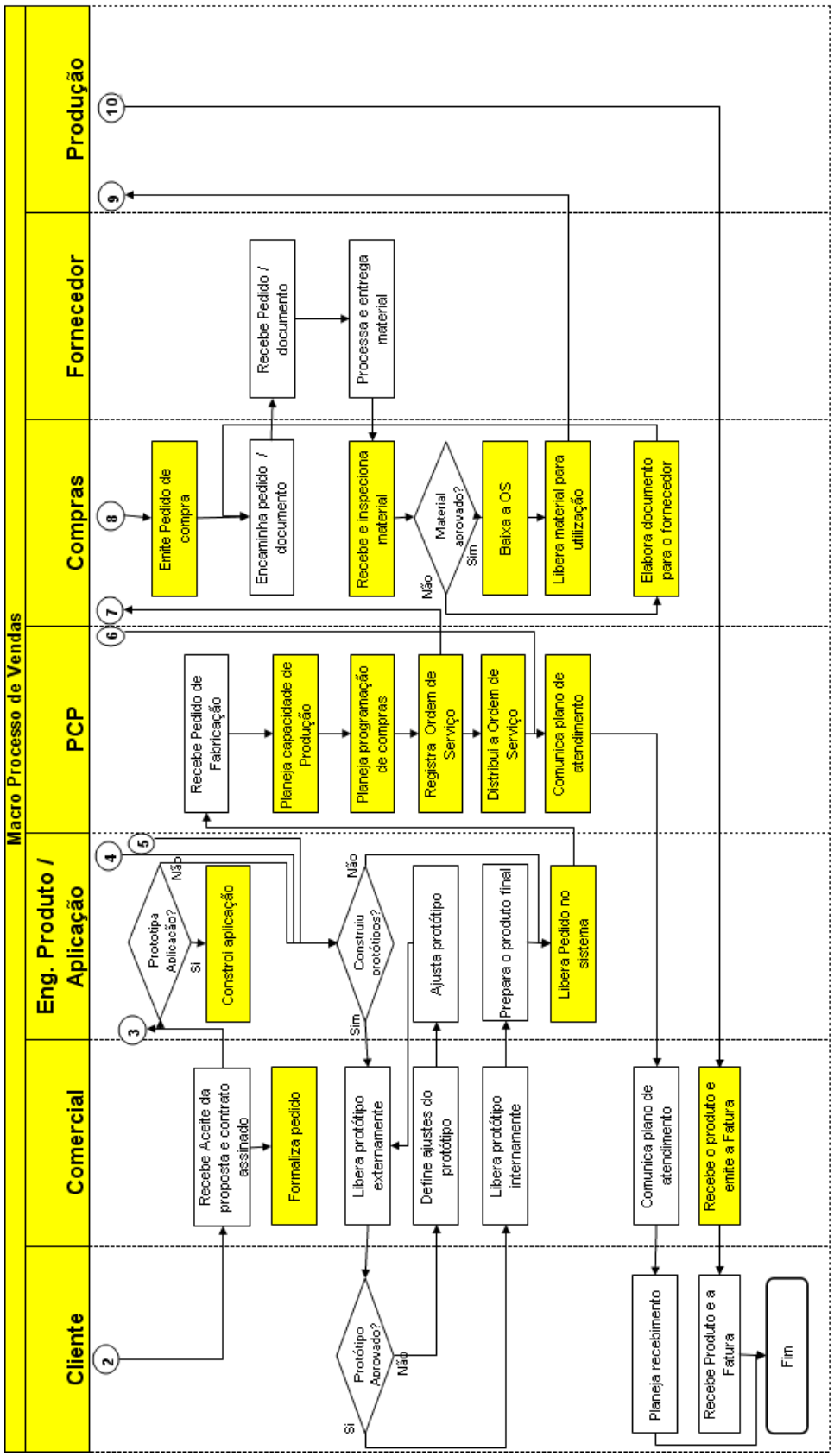


Figura 8: Macro processo de Vendas (continuação)

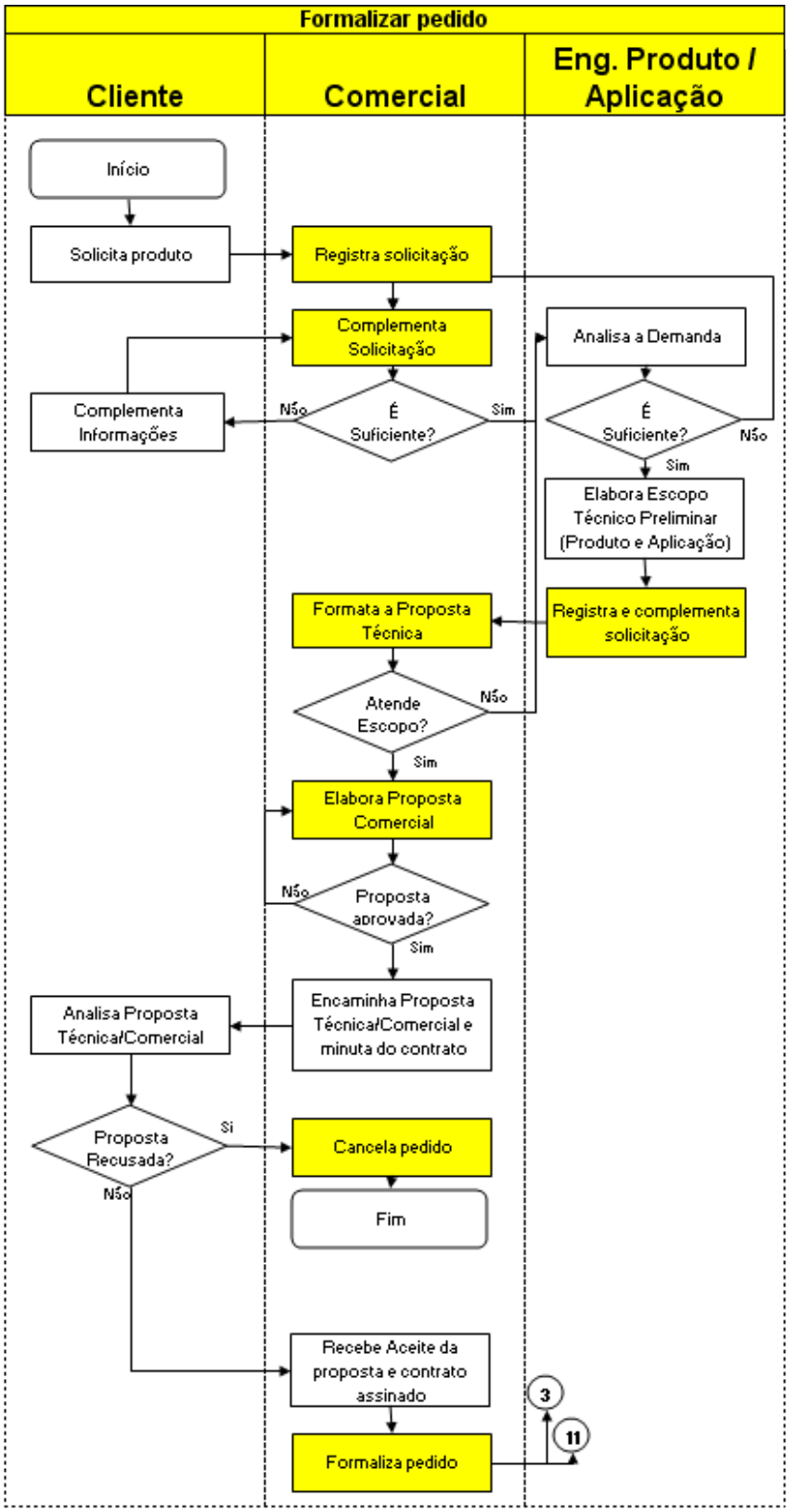


Figura 9: Processo Formalizar Pedido

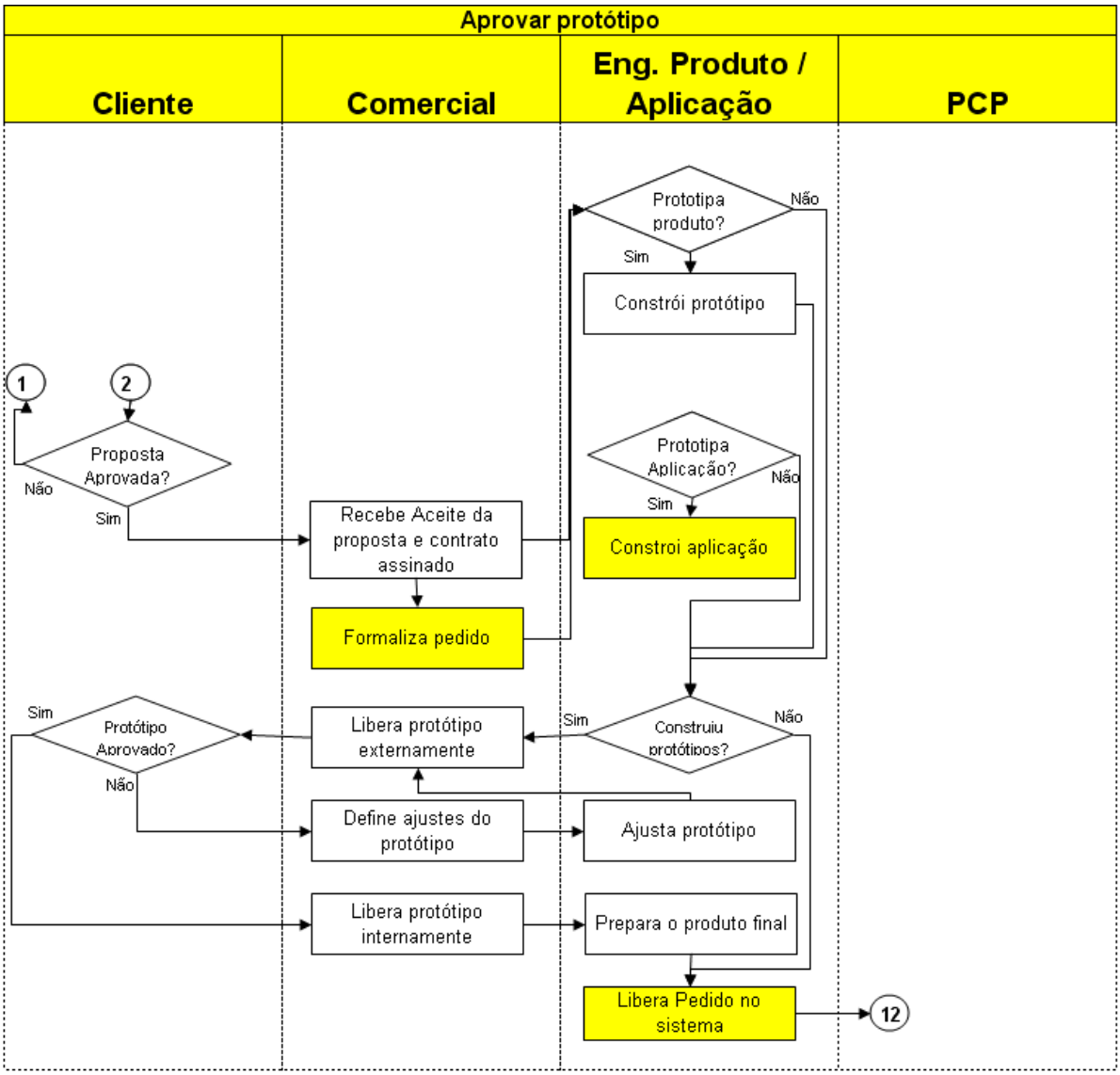


Figura 10: Processo Aprovar Protótipo

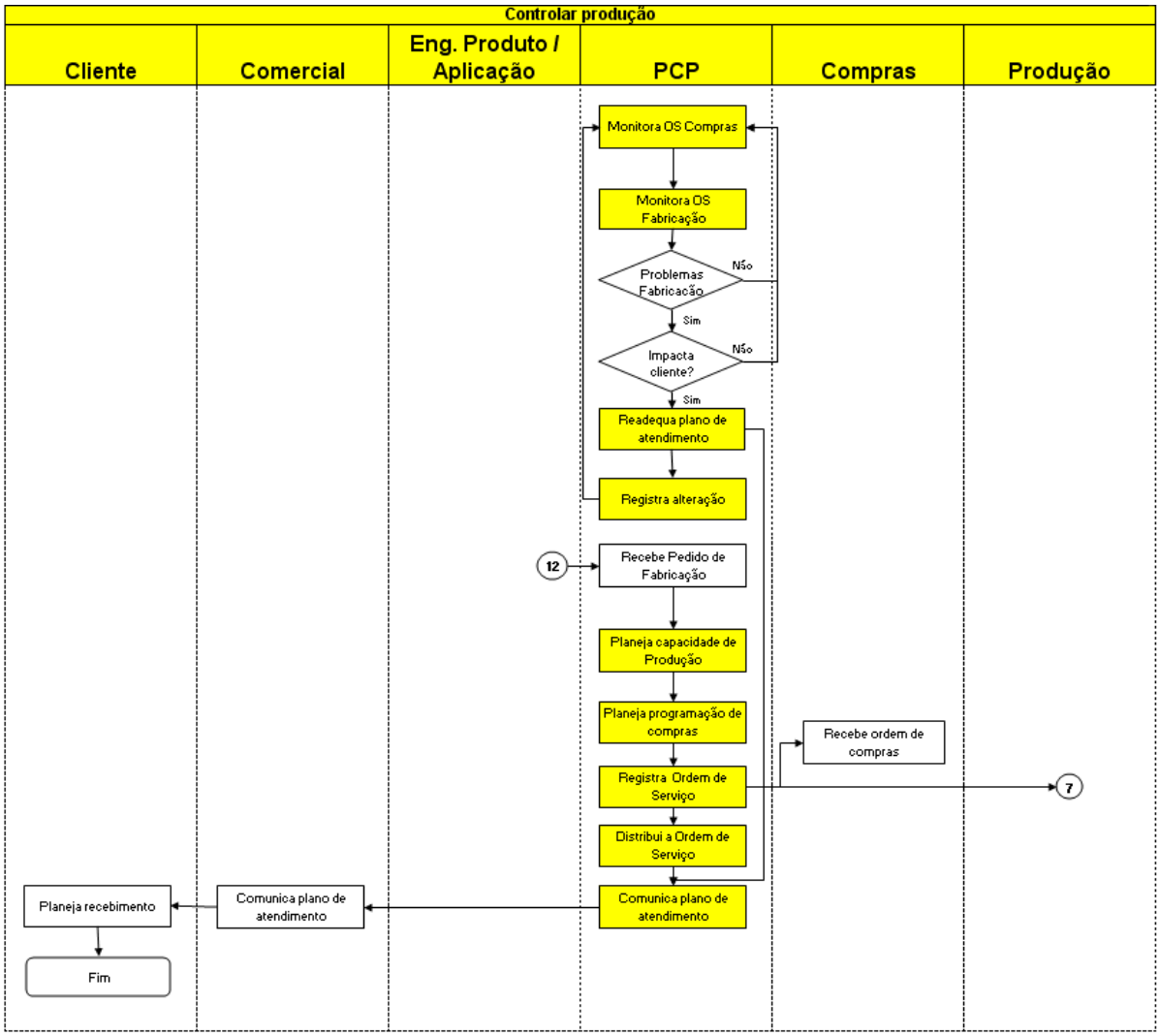


Figura 11: Processo Controlar Produção

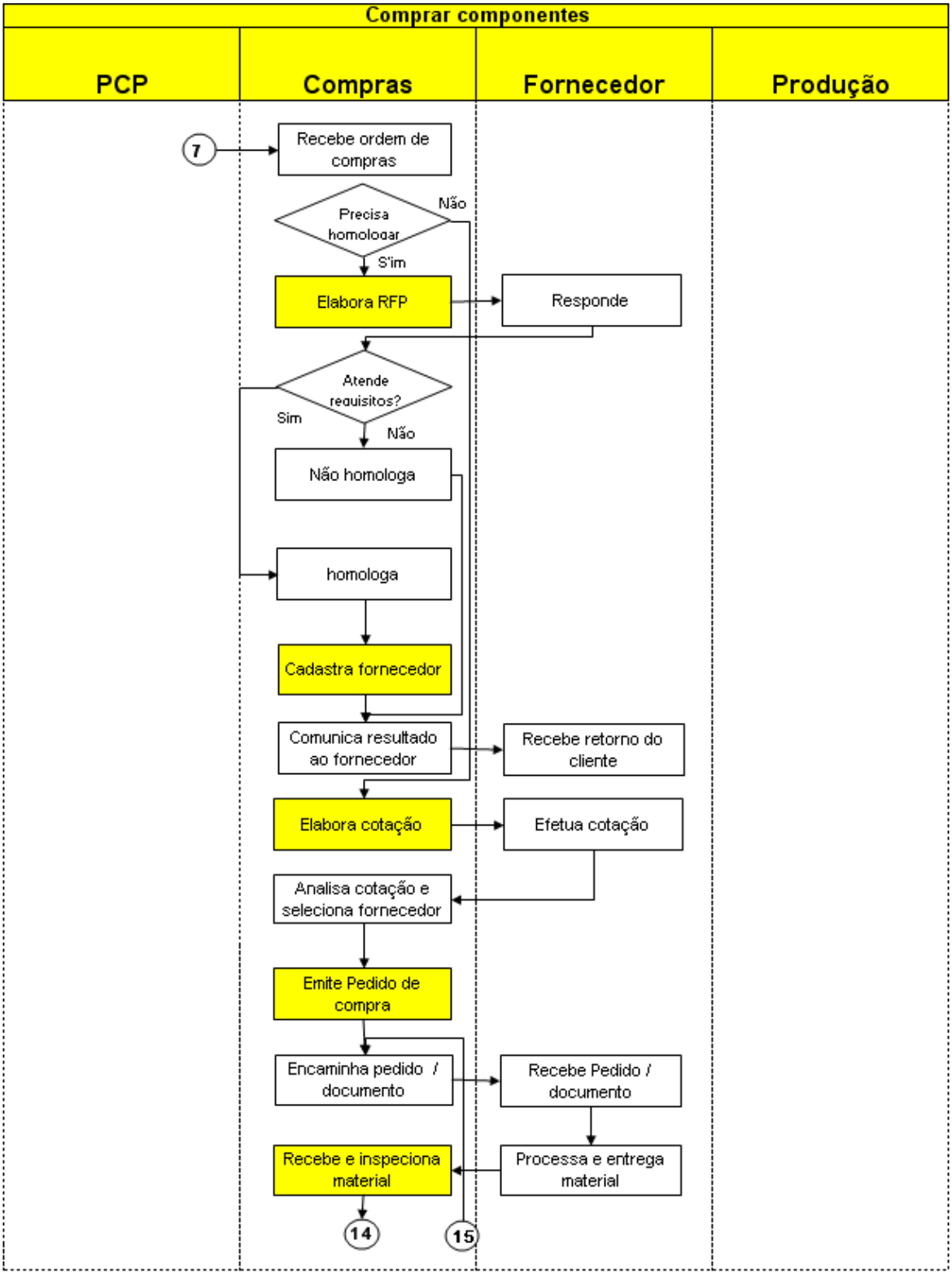


Figura 12: Processo Comprar Componentes

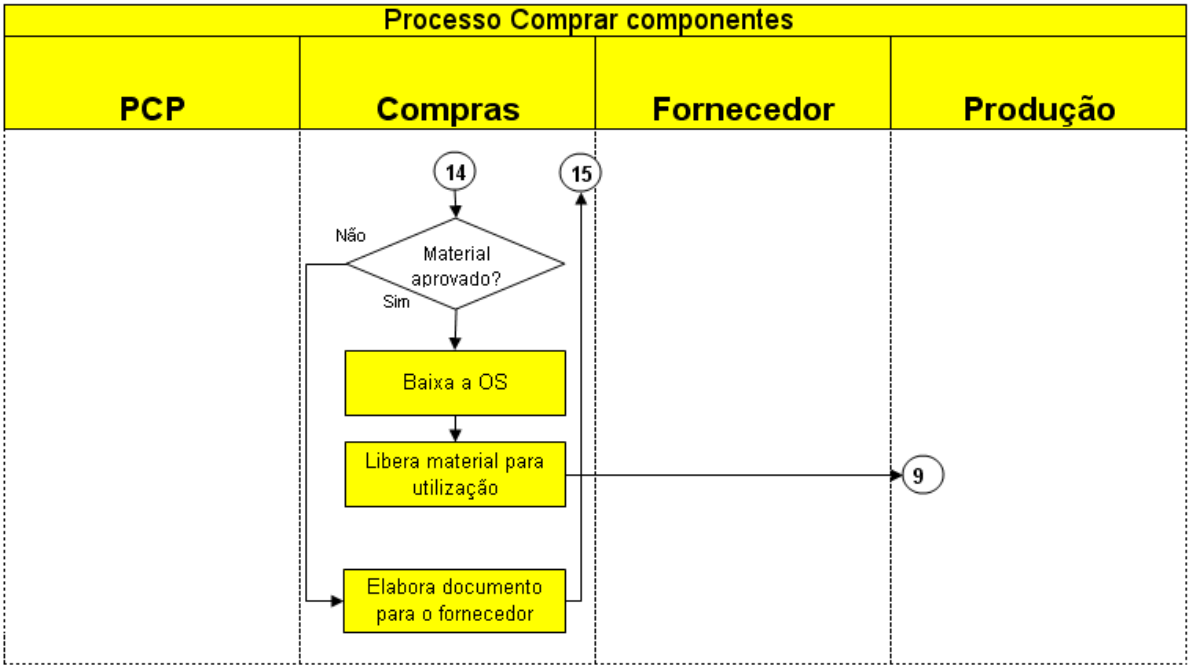


Figura 13: Processo Comprar Componentes (continuação)

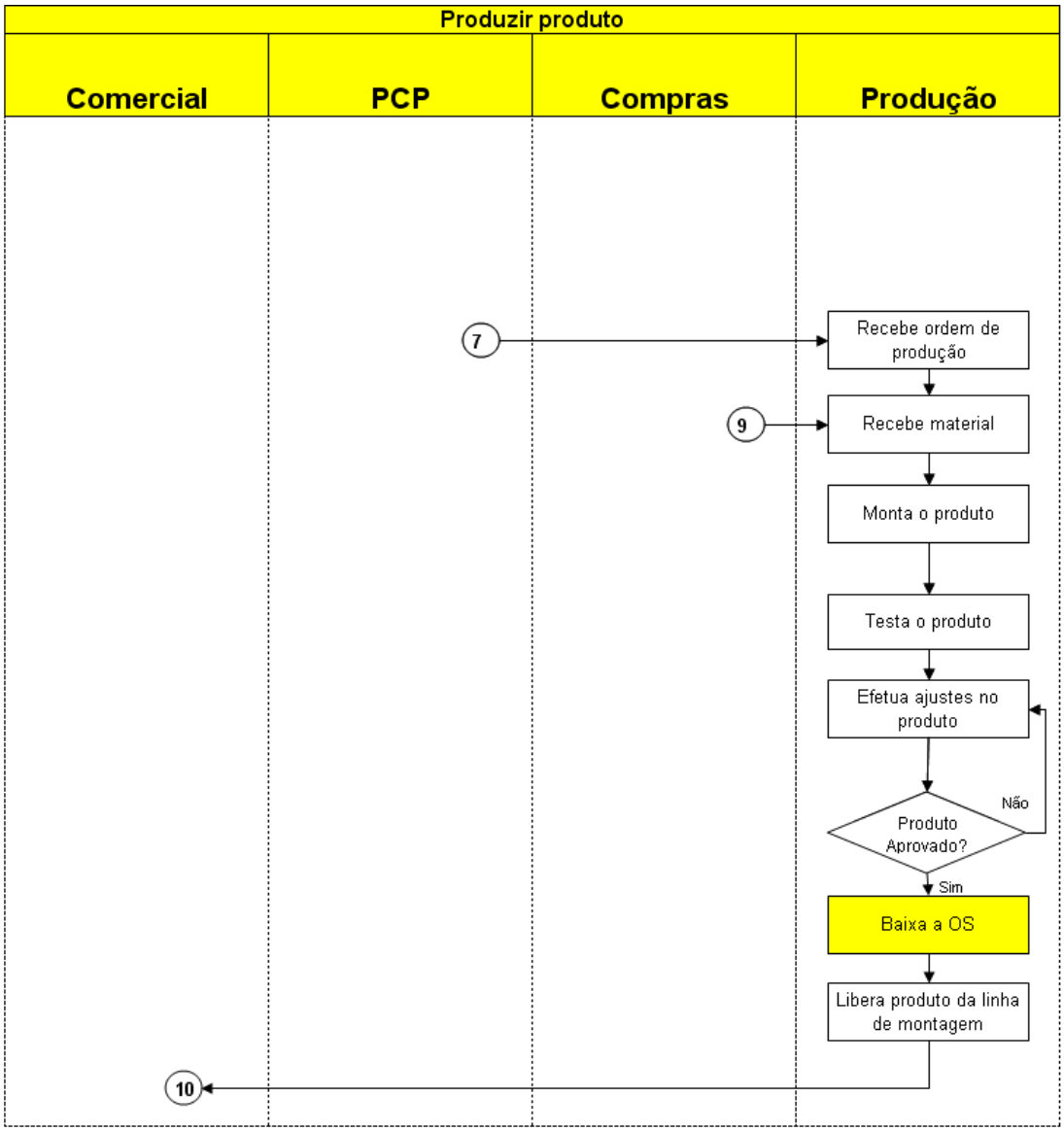


Figura 14: Processo Produzir Produto

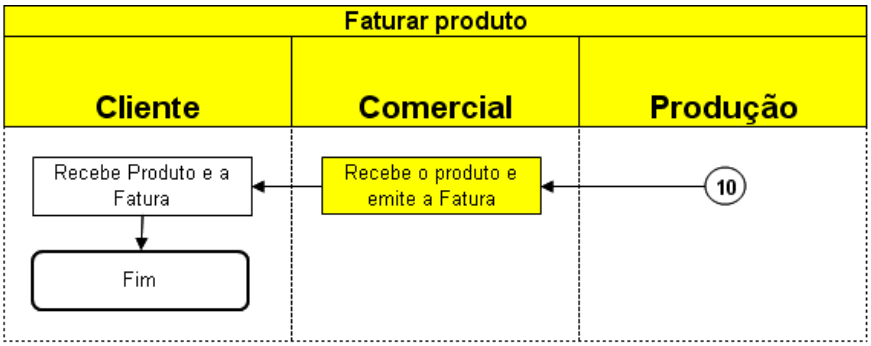


Figura 15: Processo Faturar Produto

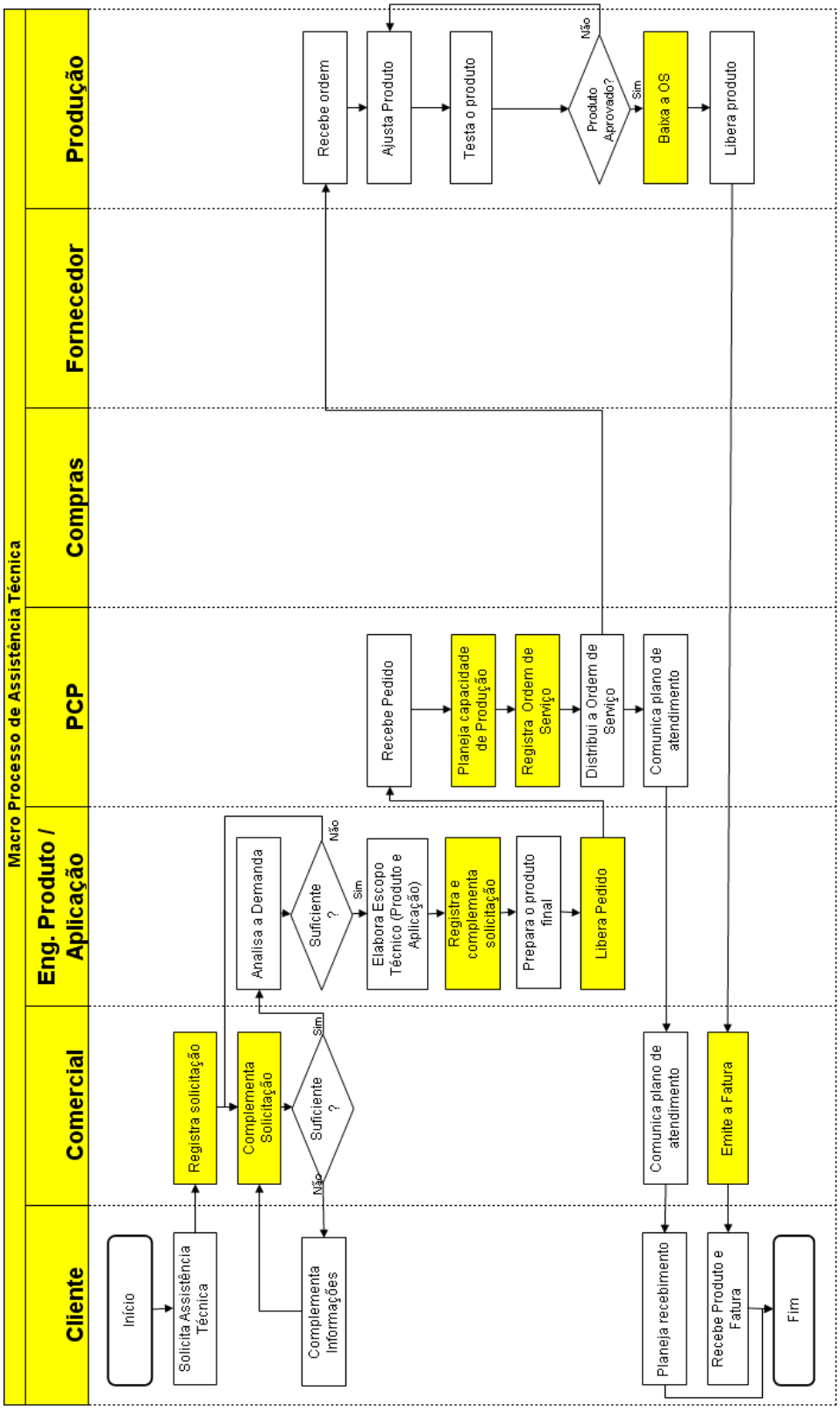


Figura 16: Macro Processo de Assistência Técnica

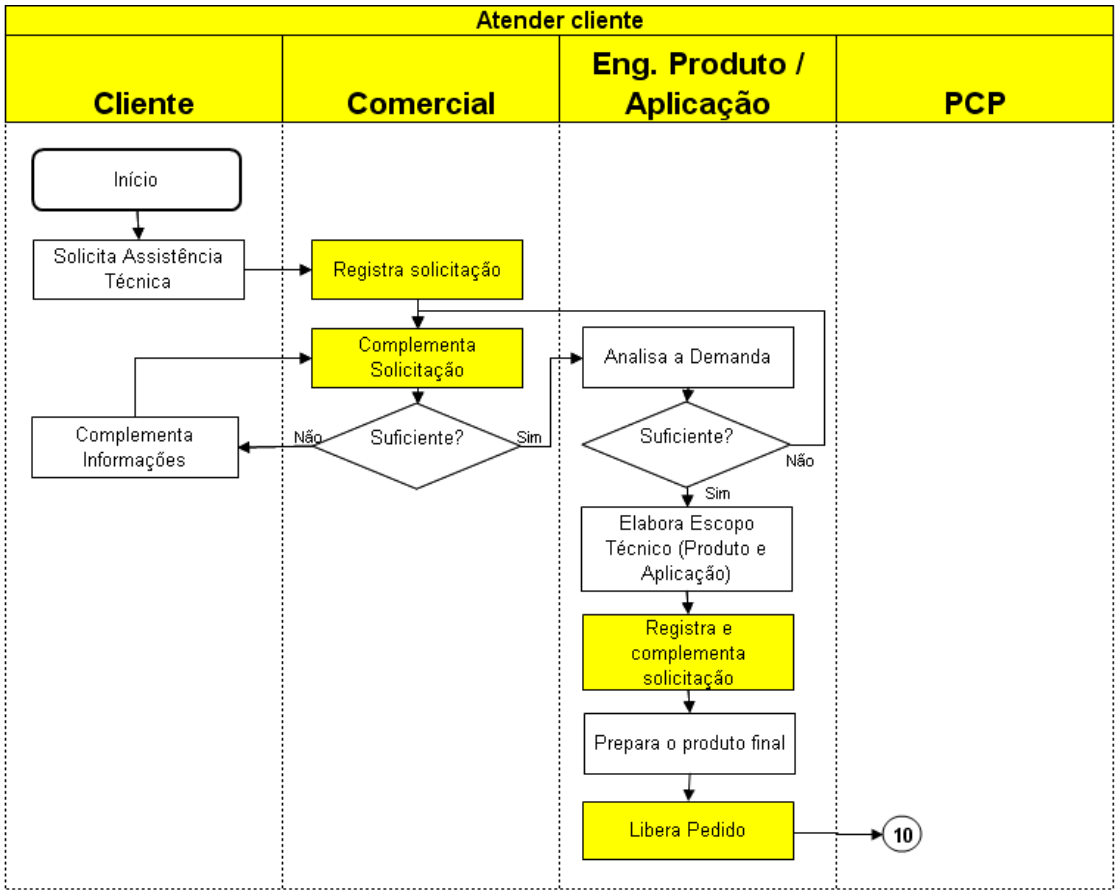


Figura 17: Processo Atender Cliente

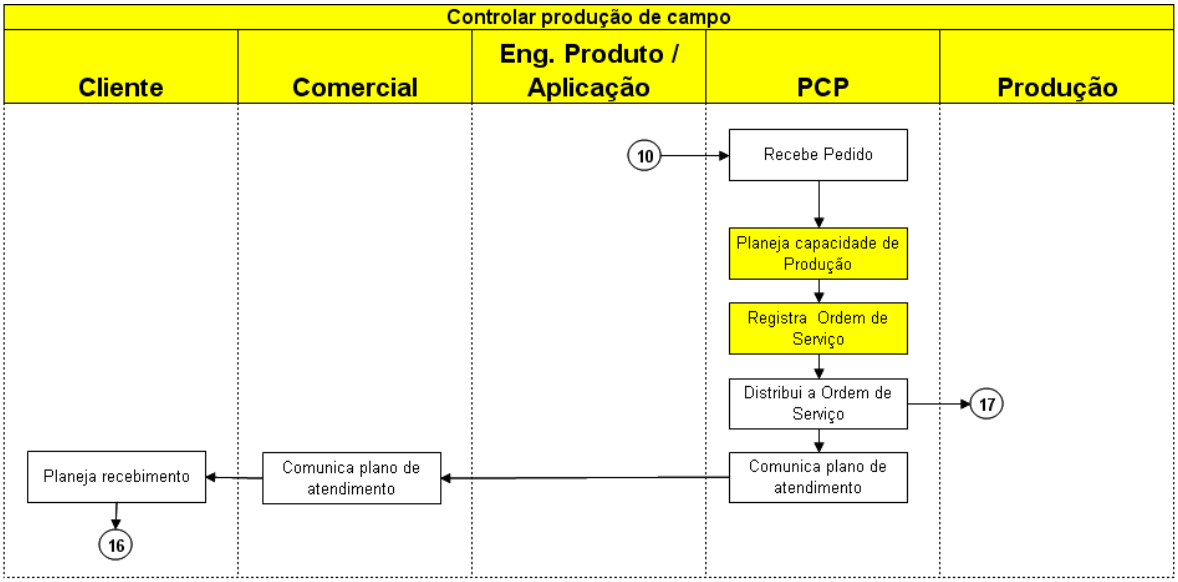


Figura 18: Processo Controlar Produção de Campo

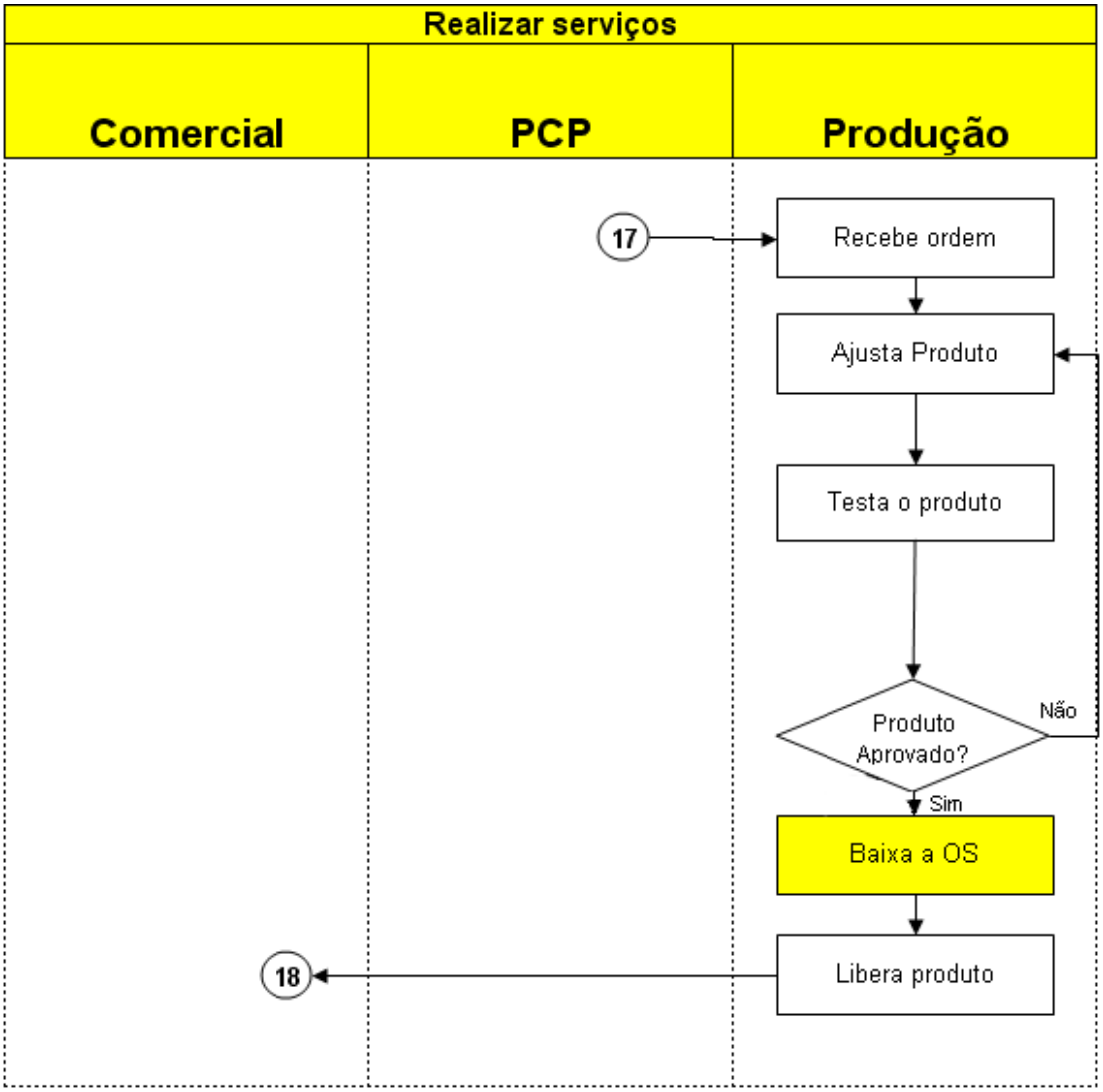


Figura 19: Processo Realizar Serviços

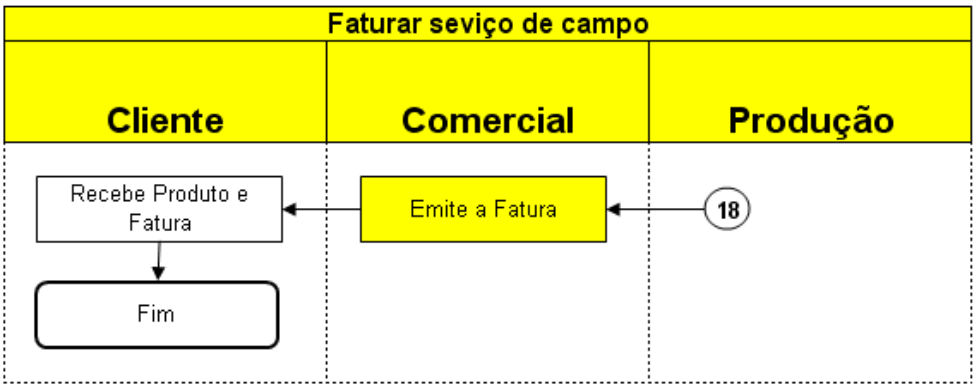


Figura 20: Processo Faturar Serviço de Campo

5 CRONOGRAMA DAS ATIVIDADES DE SEGURANÇA DE INFORMAÇÃO

Com base nas informações levantadas até aqui, que serviram para o CSO conhecer mais de perto a situação e as características da empresa, foi elaborado um cronograma, conforme apresentado na Figura 21.

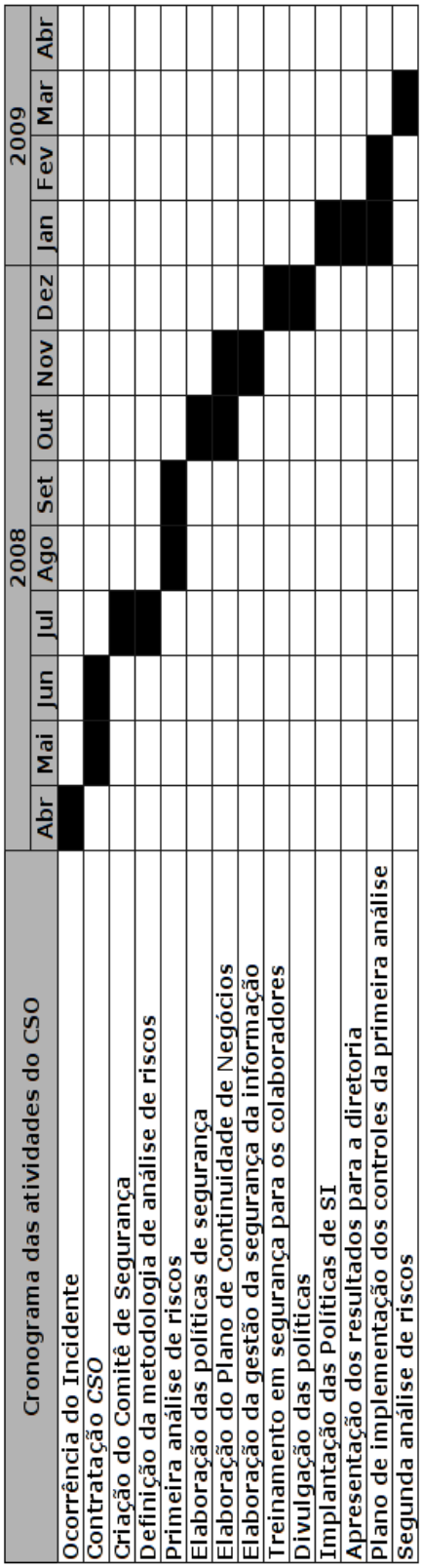


Figura 21: Cronograma das atividades de SI

6 METODOLOGIA DA ANÁLISE DE RISCOS

O processo de análise de riscos pode ser iniciado após o término da identificação de processos e ativos. A análise de riscos tem por objetivo avaliar as vulnerabilidades às quais a empresa está exposta e o impacto que a exploração de uma ou mais vulnerabilidades por um agente de ameaça pode provocar na execução de sua missão.

A análise de riscos, além de ser de vital importância para a missão da empresa, também permite elaborar estratégias para o controle dos riscos.

A metodologia da M2FE segue alguns passos bem definidos de forma que, se realizada mais de uma vez sobre os mesmos ativos, os resultados serão semelhantes.

Nos próximos itens serão apresentados os critérios da análise de riscos e as etapas necessárias para a avaliação de cada ativo.

6.1 Identificação dos ativos críticos

A segurança da informação é um processo contínuo e, como a análise de riscos é parte deste processo, ela deve ser realizada periodicamente e deve ser iniciada com a definição de quais serão os alvos da análise. Como o processo de segurança na M2FE está em sua fase inicial, os ativos serão selecionados para avaliação de acordo com a sua criticidade para o negócio.

Para identificar os ativos críticos, primeiramente devem ser obtidos (ou elaborados se ainda não existirem documentos sobre os mesmos) os processos da organização.

Uma vez conhecidos os processos, deve-se elaborar o diagrama de inter-relacionamento entre eles, fornecendo assim uma visão global de como as informações trafegam dentro da organização. Esta fase da análise necessita da participação dos responsáveis e especialistas de cada área.

A partir do diagrama de processos deve-se verificar quais sistemas são utilizados em cada processo.

Uma vez identificados os sistemas, deve-se identificar quais ativos suportam estes sistemas. Esta informação pode ser obtida junto ao departamento de tecnologia da informação ou através da verificação das configurações de cada um dos sistemas.

Durante esta fase de mapeamento (processos, sistemas e ativos) pode ser elaborado um diagrama contendo os processos na parte superior, os sistemas logo abaixo e, por fim, os ativos que dão suporte aos sistemas. Neste diagrama, os processos devem ser interligados aos sistemas. Da mesma forma, os sistemas devem ser interligados aos ativos que os suportam. O resultado final é o mapeamento de processos, sistemas e ativos. O diagrama pode ser elaborado de várias formas e a Figura 22 apresenta um exemplo.

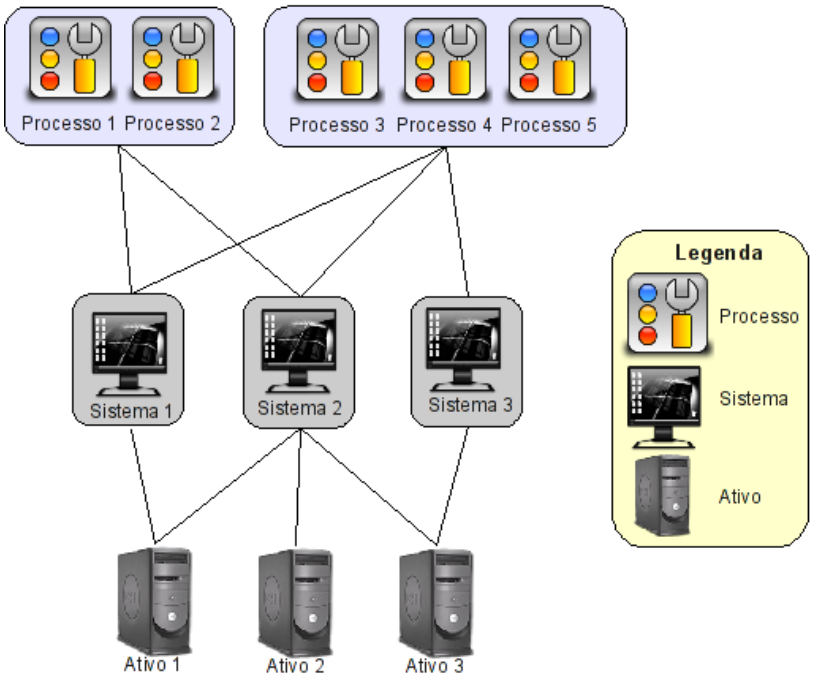


Figura 22: Exemplo de diagrama de interação entre processos, sistemas e ativos

Identificados os principais processos, verificam-se quais sistemas e ativos os suportam. Para permitir o mapeamento direto entre os processos e os ativos, deve ser elaborada uma tabela conforme modelo apresentado na Tabela 4 (Modelo de tabela de mapeamento entre processos e ativos).

Tabela 4: Modelo de tabela de mapeamento entre processos e ativos

	Ativo 1	*Ativo 2*	*Ativo 3*	*Ativo 4*	*Ativo 5*	*Ativo 5*	*Ativo 6*	*Ativo 7*	*Ativo 8*
Processo 1	x	x	x	x	x	x	x		
Processo 2	x	x	x	x	x	x	x		
Processo 3		x	x						

A partir dessa tabela identificamos os ativos que suportam os processos. Todos os ativos que aparecem nesse mapeamento são potenciais ativos críticos, porém deve-se levar em consideração que determinadas tarefas podem ser executadas de formas alternativas em caso

de contingência, por exemplo, manualmente. Os ativos mais críticos são aqueles que suportam os maiores números de processos.

Da lista de ativos obtida no mapeamento, devem ser selecionados os que serão alvos da análise de riscos. Para tanto, deve-se listar todos os ativos numa tabela conforme o modelo apresentado na Tabela 5 (Modelo de tabela de justificativa de criticidade de ativo) e indicar quais ativos serão alvos da análise de riscos, sendo que os que não forem selecionados, devem obrigatoriamente ter uma justificativa do motivo de sua exclusão.

Tabela 5: Modelo de tabela de justificativa de criticidade de ativo

Ativo	***Crítico***	***Justificativa***
Servidor de *e-mail*	Não	Em contingência as mensagens poderão ser enviadas via fax, correios e outros meios.
Servidor *Proxy*	Não	Em contingência os usuários poderão acessar a *Internet* diretamente

Na Coluna **Ativo** descreve-se o nome do ativo, na Coluna **Crítico** responde-se sim ou não para a execução da análise de risco e na Coluna **Justificativa** descreve-se o motivo pelo qual o ativo não será alvo da análise de risco, caso ele tenha sido considerado não crítico.

Além dos ativos críticos, a análise de riscos deve ser aplicada aos seguintes itens:

- *Data center*
- Rede
- Segurança física

6.2 Riscos e Controles

Esta metodologia utiliza-se de listas (*checklists*) de controles a serem verificados e implementados nos ativos de acordo com as suas características. Estas listas de controles

revelam as vulnerabilidades expostas pelo ativo e os riscos aos quais ele está sujeito. Uma vez implementados os controles, os riscos são controlados ou mitigados.

Estes *checklists* representam o ponto de partida da análise de riscos de cada um dos ativos. É a partir deles que as demais informações serão determinadas.

Uma vez definidos os ativos a serem avaliados, devem ser levantadas as suas características básicas como por exemplo, o sistema operacional e os serviços ou sistemas que ele suporta. Estas informações são essenciais para a seleção das listas de controles (*checklists*) a serem empregadas na avaliação do ativo. Observe que um único ativo pode utilizar mais de um *checklist*. Por exemplo, num ativo do tipo servidor aplica-se um *checklist* de controles a serem verificados no sistema operacional e outro relacionado à aplicação executada neste servidor.

Independente de quantos *checklists* forem utilizados para cada ativo, sempre serão apresentados resumos de quantidade de controles, custos e investimentos, que oferecem uma visão geral do estado em que se encontra o ativo.

Assim como a análise de riscos deve ser executada periodicamente (a cada ano, por exemplo), os *checklists* também devem ser atualizados em função das novas ameaças que surgem e das características dos serviços disponibilizados pelos ativos. As atualizações dos *checklists* devem ser baseadas em fontes bem conhecidas, como os fabricantes dos produtos e organizações voltadas à segurança de sistemas.

A Tabela 6 (Exemplo de *checklist*) apresenta um exemplo de *checklist*, com um número reduzido de itens. Usaremos os nomes das colunas como referência no preenchimento do *checklist*. Todos utilizado para a análise estão disponíveis no Anexo A.4.

Tabela 6: Exemplo de *checklist*

NOME DO ATIVO		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Versão do *Netfilter* deve ser a versão estável mais atual	2	TEC						
2	Os registros de *log* do *Netfilter* devem ser analisados diariamente	1	TEC						
3	Os arquivos de *log* devem ser rotacionados semanalmente	2	TEC						
4	O *backup* das regras do *Netfilter* deve ser realizado semanalmente	2	TEC						
5	As regras de filtragem devem ser criadas na ordem correta (e testadas)	8	TEC						

A primeira coluna da primeira linha do *checklist* deve ser preenchida com o nome do ativo. Esta coluna é sub-dividida em duas colunas: a primeira enumera os itens do *checklist* e a segunda descreve os controles a serem verificados.

A terceira coluna (**Tipo ameaça**) identifica o tipo da ameaça, baseado na norma (NBR ISO/IEC 27005:2008, 2008), e apresentados na Tabela 7 (Tipos de Ameaça). Esta coluna

também deve ser preenchida no ato da criação do *checklist*, visto que esta informação está vinculada ao controle e não à situação do ativo.

Tabela 7: Tipos de Ameaça

Tipos de ameaças	
#	***Descrição***
1	Ações não autorizadas
2	Comprometimento da informação
3	Criminoso digital
4	Dano físico
5	Distúrbio causado por radiação
6	Espionagem industrial
7	Eventos naturais
8	Falhas técnicas
9	*Cracker*
10	Paralisação de serviços essenciais
11	Pessoal interno
12	Terrorista

A quarta coluna (**Tipo vuln.**) classifica o tipo de vulnerabilidade, também baseada na norma (NBR ISO/IEC 27005:2008, 2008), relacionado à ameaça que é alvo do controle. Esta coluna também deve ser preenchida no ato da criação do *checklist* e os valores possíveis são descritos na Tabela 8 (Tipos de vulnerabilidades).

Tabela 8: Tipos de vulnerabilidades

Tipos de vulnerabilidades	
AMB	Ambiental
HUM	Humana
TEC	Tecnológica

6.2.1 Situação atual do controle

O preenchimento do *checklist* inicia-se pela coluna 5 (**Implementado**). Esta coluna deve ser preenchida com um dos valores apresentados na Tabela 9 (Situação atual).

Tabela 9: Situação atual

Situação atual do controle	
#	***Descrição***
S	Controle implementado
N	Controle não implementado
N/A	Controle não aplicável

Esta coluna deve ser preenchida cuidadosamente, pois é ela que define se o item em questão deve ou não ser contabilizado no cálculo do risco: apenas os itens não implementados serão considerados.

Um controle pode ser classificado como N/A (não aplicável) quando o controle não possuir aplicação direta sobre o ativo. Por exemplo, um controle do tipo 'Habilitar o SYSKEY', que exige que seja digitada uma senha para que o sistema operacional seja iniciado, não é interessante nos casos em que não seja possível a intervenção humana na ocorrência de queda e restabelecimento de energia. Em casos como este o controle não deve

ser implementado. Os controles classificados como N/A no *checklist* são simplesmente ignorados em todos os cálculos posteriores.

6.2.2 Custo estimado e investimento

Uma vez determinada a situação dos itens do *checklist*, deve-se estimar o custo e o investimento necessários para a implementação dos controles não implementados no ativo.

Na coluna de custo (**Custo estim. HH**) apresentado na Tabela 6 (Exemplo de *checklist*) deve ser estimado o tempo, em termos de horas/homem, necessário para a implementação do controle. Se o item de controle em questão estiver implementado, o preenchimento deste campo é opcional.

Já a coluna de investimento (**Investimento estim. R$**) deve ser preenchida com o valor, em Reais, estimado dos insumos necessários, excetuando-se a mão-de-obra. Por exemplo, o custo de aquisição de um *hardware* ou *software* necessário para a implementação do item do *checklist* deve ser lançado nesta coluna. Se o item de controle em questão estiver implementado, o preenchimento deste campo é opcional.

6.2.3 Probabilidade

A Coluna **Prob.** da Tabela 6 (Exemplo de *checklist*) identifica a probabilidade de uma ameaça explorar uma vulnerabilidade relacionada ao controle em questão. Esta coluna deve ser preenchida com um dos valores de nível descritos na Tabela 10 (Critérios de qualificação da probabilidade). Estes critérios foram baseados nos critérios definidos por (STONEBURNER; GOGUEN; FERINGA, 2002, p.21).

Tabela 10: Critérios de qualificação da probabilidade

Probabilidade		
Nível	***Significado***	***Definição do critério***
A	**Alto**	O risco é iminente, pois o controle não está implementado. Exemplo: o serviço *telnet* deve ser desabilitado. No serviço *telnet*, a comunicação não é cifrada, permitindo que as senhas de acesso sejam facilmente capturadas na rede.
M	**Médio**	A probabilidade da ocorrência da exploração da vulnerabilidade é razoável e os controles existentes atualmente podem impedir a exploração, mas não são suficientemente eficientes para prevenir totalmente a exploração da vulnerabilidade. Exemplo: ajuste a máscara de gravação de arquivos para 0770. Em sistemas Unix/Linux, este ajuste restringe o acesso ao dono do arquivo e ao grupo especificado. Desta forma, se ocorrer uma invasão com os privilégios de usuário, apenas os arquivos acessíveis por este usuário serão comprometidos.
B	**Baixo**	A probabilidade da ocorrência da exploração da vulnerabilidade é pequena ou os controles existentes impedem significativamente a sua exploração. Exemplo: desabilitar o desligamento do computador através da sequência CTRL-ALT-DEL. Se o computador estiver dentro de uma área com controle de acesso, como um *data center*, por exemplo, a probabilidade desta sequência de teclas ser pressionada é muito baixa.

6.2.4 Impacto

A Coluna **Impacto** da Tabela 6 (Exemplo de *checklist*) deve ser preenchida com o nível do impacto ocasionado caso a vulnerabilidade referente ao controle descrito no *checklist* venha a ser explorada. O nível de impacto deve ser preenchido com um dos valores indicados

na Coluna **Nível** da Tabela 11 (Critérios de qualificação do impacto). Estes critérios foram baseados nos definidos por (STONEBURNER; GOGUEN; FERINGA, 2002, p.23).

Tabela 11: Critérios de qualificação do impacto

Impacto		
Nível	***Significado***	***Definição do critério***
A	**Alto**	A exploração da vulnerabilidade pode resultar em um ou mais dos seguintes itens: ● Perda dos **principais** ativos ou recursos. ● Violação, dano ou impedimento **significativo** a realização da missão da organização, reputação ou interesse. ● Ameaça à vida. Exemplo: O acesso físico ao servidor deve ser restrito e controlado.
M	**Médio**	A exploração da vulnerabilidade pode resultar em um ou mais dos seguintes itens: ● Perda de ativos ou recursos. ● Violação, dano ou impedimento a realização da missão da organização, reputação ou interesse. ● Danos ou ferimentos às pessoas. Exemplo: Somente os responsáveis pela segurança poderão liberar acesso aos usuários.

Impacto		
Nível	***Significado***	***Definição do critério***
B	**Baixo**	A exploração da vulnerabilidade pode resultar em um ou mais dos seguintes itens: ● Perda de algum ativo ou recursos. ● Ameaça à missão, reputação ou interesse da organização. Exemplo: Habilitar o registro de acesso dos usuários.

6.2.5 Risco

A última coluna (**Risco**) da Tabela 6 (Exemplo de *checklist*) deve ser preenchida com o nível do risco, que deve ser calculado usando-se os valores preenchidos nas colunas de probabilidade (**Prob.**) e impacto (**Impacto**), conforme descrito a seguir. Normalmente, o risco é o produto da probabilidade versus o impacto (**Risco = Probabilidade x Impacto**), mas como esta metodologia é essencialmente qualitativa, o nível do risco deve ser determinado usando-se a Tabela 12 (Qualificação do risco). Estes critérios foram baseados naqueles definidos por (STONEBURNER; GOGUEN; FERINGA, 2002, p.25).

Tabela 12: Qualificação do risco

Risco		***Probabilidade***		
		Alta	***Média***	***Baixa***
Impacto	**Alto**	Alto	Alto	Médio
	Médio	Alto	Médio	Baixo
	Baixo	Médio	Baixo	Baixo

6.3 Resumo dos riscos

Uma vez finalizados os cálculos dos riscos, deve ser elaborado um resumo dos riscos relacionados ao ativo. Este resumo é realizado em duas partes, a saber:

- **Resumo dos riscos por intensidade.** Este resumo é composto por uma tabela contendo o número de ocorrências dos riscos classificados de acordo com a intensidade do risco. Uma vez elaborada a tabela com os dados, um gráfico deve ser produzido a partir dos dados da tabela.

- **Resumo dos riscos por tipo de vulnerabilidade.** Este resumo é composto por uma tabela contendo o número de ocorrências dos riscos agrupados pelo tipo de vulnerabilidade relacionada. Uma vez elaborada a tabela com os dados do resumo, um gráfico deve ser produzido a partir desta tabela.

O resumo dos riscos por intensidade deve ser montado baseado no preenchimento de uma tabela seguindo o modelo apresentado na Tabela 13 (Modelo de resumo dos riscos por intensidade).

Tabela 13: Modelo de resumo dos riscos por intensidade

Ativo ***Resumo dos riscos por intensidade***			
Nível		***Ocorrências***	***%***
A	**Alto**		
M	**Médio**		
B	**Baixo**		

Para preencher a tabela, primeiramente deve-se substituir o texto **Ativo** contido na primeira linha pelo nome ou identificador do ativo.

A Coluna **Ocorrências** deve ser preenchida com número de ocorrências de riscos de nível alto, médio e baixo obtidos de todos os *checklists* aplicados ao ativo. A coluna de percentual (%) deve ser preenchida com os valores percentuais (em relação ao número total de ocorrências) referentes aos níveis alto, médio e baixo preenchidos na Coluna **Ocorrências**. Para determinar o valor percentual de cada item, deve-se determinar o número total de ocorrências, que é dado por:

$$Total = OcorrênciasNívelAlto + OcorrênciasNívelMédio + OcorrênciasNívelBaixo$$

Uma vez determinado o número total de ocorrências, determina-se o valor percentual de risco da seguinte forma:

$$PercentualAlto = \frac{OcorrênciasNívelAlto}{Total} * 100$$

$$PercentualMédio = \frac{OcorrênciasNívelMédio}{Total} * 100$$

$$PercentualBaixo = \frac{OcorrênciasNívelBaixo}{Total} * 100$$

Uma vez preenchida a tabela, deve ser produzido um gráfico de barras contendo o número de ocorrências dos riscos classificados por intensidade, conforme exemplo apresentado na Figura 23.

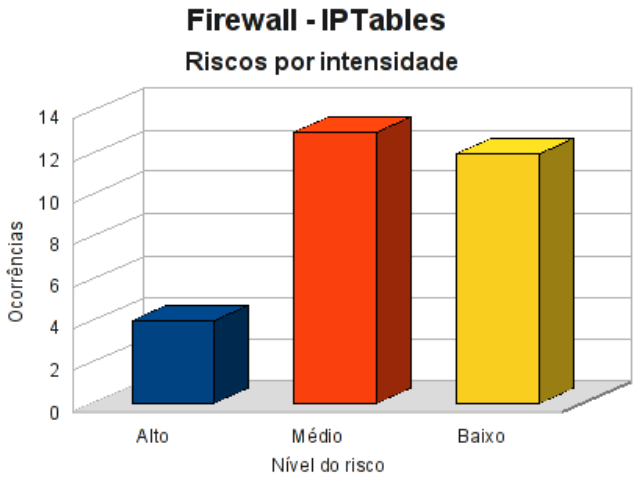


Figura 23: Exemplo de gráfico de riscos por intensidade

O resumo dos riscos por tipo de vulnerabilidade agrupa as ocorrências dos riscos de acordo com o tipo de vulnerabilidade. Para elaborar este resumo deve-se agrupar e contar todos os itens não implementados de todos os *checklists* aplicados ao ativo conforme o tipo de vulnerabilidade e o nível do risco. Os resultados obtidos devem ser usados para preencher a tabela deste resumo, conforme modelo apresentado na Tabela 14 (Modelo de resumo dos riscos por tipo de vulnerabilidade). O texto **Ativo** da primeira linha da tabela deve ser substituído pelo nome ou identificação do ativo em questão.

Tabela 14: Modelo de resumo dos riscos por tipo de vulnerabilidade

Ativo ***Resumo dos riscos por tipo de vulnerabilidade***				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**			
M	**Médio**			
B	**Baixo**			

Uma vez preenchida a Tabela 14 (Modelo de resumo dos riscos por tipo de vulnerabilidade), estes valores devem ser exibidos num gráfico de barras contendo o número de ocorrências dos riscos por intensidade e tipo de vulnerabilidade, conforme exemplo apresentado na Figura 24.

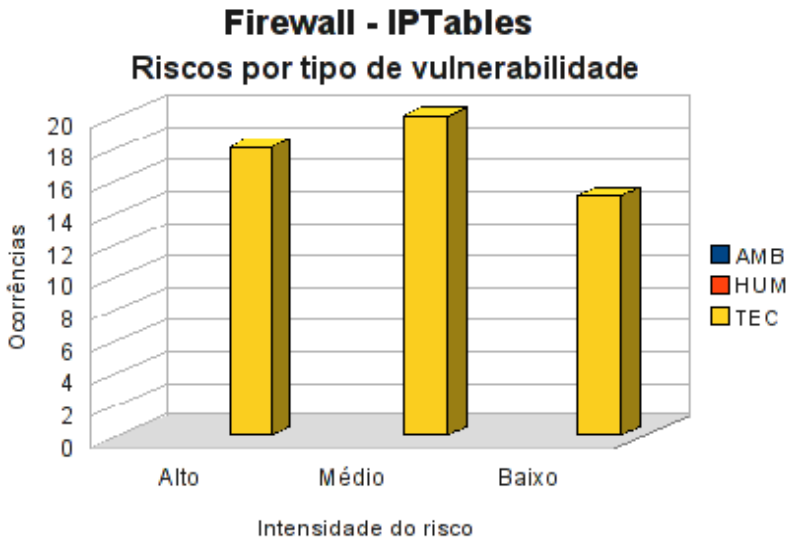


Figura 24: Exemplo de gráfico de riscos por tipo de vulnerabilidade

Este resumo é interessante pois fornece uma visão gráfica da distribuição dos riscos de acordo com o tipo de vulnerabilidade.

6.4 Conformidade com os controles

O próximo resumo consiste na verificação de quanto o ativo em questão está em conformidade com os controles especificados nos *checklists* aplicados. Esta informação é interessante pois fornece uma visão do estado do ativo no que diz respeito aos itens de segurança. Para construir este resumo usa-se a Tabela 15 (Conformidade do ativo com os controles) como referência.

Tabela 15: Conformidade do ativo com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados		
Implementados		
Total		

O preenchimento desta tabela deve ser feito da seguinte forma: conta-se o número de controles de todos os *checklists* aplicados ao ativo que não estão implementados e anota-se o valor na Coluna **Qde** referente à linha de controles não implementados. Da mesma forma, conta-se o número de controles de todos os *checklists* aplicados ao ativo que encontram-se implementados e anota-se o valor obtido na Coluna **Qde** referente à linha de controles implementados. Observe que os itens de controle cujo estado de implementação seja N/A (Não aplicável) não devem ser considerados. Somam-se os números de controles implementados e não implementados e anota-se o valor na Coluna **Qde** referente à linha denominada **Total**. Na coluna percentual (**%**), calcula-se o percentual de controles implementados e não implementados em relação ao número total de controles. Os valores percentuais devem ser calculados da seguinte forma:

$$Total = NãoImplementado + Implementado$$

$$PercentualNãoImplementado = \frac{NãoImplementado}{Total} * 100$$

$$PercentualImplementado = \frac{Implementado}{Total} * 100$$

Uma vez preenchida a tabela, elabora-se um gráfico de *pizza* contendo duas fatias: uma para os controles implementados e outra para os controle não implementados, conforme exemplo da Figura 25.

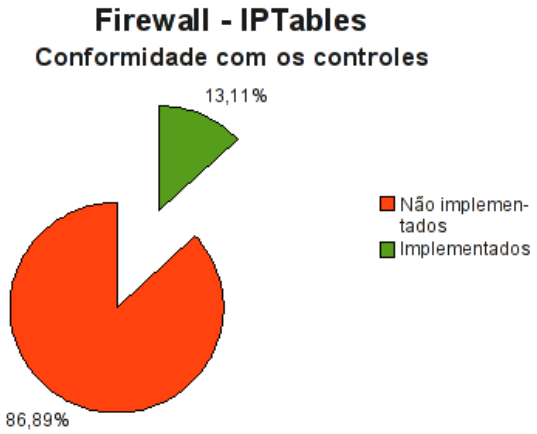


Figura 25: Exemplo de gráfico de conformidade

6.5 Investimentos necessários

Uma vez preenchidos todos os itens do *checklist*, conforme modelo apresentado na Tabela 6 (Exemplo de *checklist*), devemos calcular o custo e o investimento necessários para implementar os controles que tratam os riscos. Este cálculo deve ser feito levando-se em conta todos os itens de todos os *cheklists* aplicados ao ativo que não foram implementados. Para auxiliar no cálculo, utilizamos uma tabela conforme modelo apresentado na Tabela 16 (Modelo de custo estimado para mitigar/controlar os riscos).

Tabela 16: Custo estimado para mitigar/controlar os riscos

Ativo ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado			
Investimento			
Total a ser investido			

Para determinar o custo estimado, deve-se somar o valor do custo estimado especificado nos *checklists*, conforme modelo apresentado na Tabela 6 (Exemplo de *checklist*), para todos

os itens não implementados no ativo. O resultado desta soma é dado em horas/homem e deve ser anotado na Coluna **Total HH (R$)** referente à linha de custo estimado. Deve-se consultar valores de mercado (ou junto aos fornecedores da empresa) para obter-se o preço da hora de consultoria técnica, que deve ser expressa em Reais e anotada na linha referente ao custo, na coluna **Valor HH (R$)**. Os dois valores, **Valor HH** e **Total HH**, devem ser multiplicados e o resultado anotado na coluna **Total** referente ao custo.

Para o investimento, deve-se somar o valor do investimento especificado no *checklist*, conforme modelo apresentado na Tabela 6 (Exemplo de *checklist*), para todos os itens não implementados no ativo, anotando o resultado final na Coluna **Total** referente à linha de investimento.

Finalmente, somam-se os valores da Coluna **Total** referentes aos custos e aos investimentos e anota-se o valor na Coluna **Total**, na linha referente ao total a ser investido. Este valor consiste no montante total de investimento necessário para cobrir os custos de implementação e investimentos necessários para a mitigação ou controle dos riscos.

Um segundo resumo de investimentos deve ser realizado agrupando os valores de acordo com a intensidade do risco. O objetivo é demonstrar qual o investimento estimado necessário para mitigar os riscos de acordo com a sua intensidade. A Tabela 17 (Resumo de custos por intensidade do risco) apresenta o modelo a ser utilizado.

Tabela 17: Resumo de custos por intensidade do risco

Ativo ***Custo estimado para mitigar/controlar os riscos (por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	Alto	
M	Médio	
B	Baixo	
Total		

Para preencher a tabela e concluir o resumo de custos, deve-se agrupar os riscos de acordo com a sua intensidade (alto, médio e baixo) e realizar a soma dos valores financeiros necessários para mitigar os riscos. Esta soma deve ser realizada da seguinte forma:

1. Some os valores dos custos estimados especificados no *checklist*, conforme modelo apresentado na Tabela 6 (Exemplo de *checklist*), para todos os itens não implementados no ativo, cujo risco é alto. O resultado desta soma é dado em horas/homem e deve ser multiplicado pelo valor da hora de consultoria técnica já anotado na tabela de custo estimado para mitigar os riscos na Coluna **Total HH (R$)**. Anote este valor.

2. Some os valores de investimento especificados no *checklist*, conforme modelo apresentado na Tabela 6 (Exemplo de *checklist*), para todos os itens não implementados no ativo, cujo risco é alto. Anote este valor.

3. Some os dois valores obtidos nos passos 1 e 2 e anote na Coluna **Custo + Investimento (R$)** na linha referente ao risco de alta intensidade.

4. Repita os passos 1, 2 e 3 para os riscos de média e baixa intensidade e anote os valores nas respectivas colunas.

5. Finalmente, some todos os valores para os riscos alto, médio e baixo e anote na linha de total.

6.6 Resumo Executivo

O resumo executivo finaliza a análise de riscos e é constituído por duas partes: um resumo geral de conformidade dos ativos com os controles e um resumo dos custos e investimentos necessários para mitigar ou controlar os riscos encontrados em cada ativo.

O resumo de conformidade geral dos ativos com os controles é baseado nas informações contidas nas tabelas de conformidade de cada ativo. Para construir este resumo usa-se a Tabela 18 (Resumo geral de conformidade com os controles) como referência.

Tabela 18: Resumo geral de conformidade com os controles

Resumo geral de conformidade com os controles		
Controle	***Qtde.***	***%***
Não implementados		
Implementados		
Total		

Esta tabela deve ser preenchida da seguinte forma:

- Some todos os controles não implementados contidos nas tabelas de conformidade com os controles de cada ativo e anote o resultado na coluna referente à quantidade de controles não implementados na Tabela 18 (Resumo geral de conformidade com os controles).
- Faça o mesmo procedimento para os controles implementados.
- Some a quantidade de controles implementados e não implementados e anote o valor na linha de total.
- Calcule o percentual de controles implementados e não implementados em relação ao número total de controles verificados.

Uma vez preenchida a tabela, elabora-se um gráfico de *pizza* contendo duas fatias: uma para os controles implementados e outra para os controle não implementados, conforme exemplo da Figura 26.

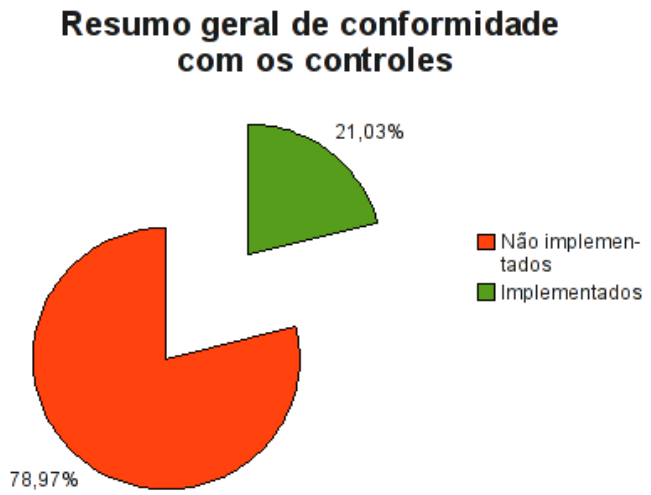


Figura 26: Exemplo de gráfico de resumo geral de conformidade

O resumo executivo dos custos e investimentos necessários deve ser elaborado utilizando-se a Tabela 19 (Exemplo de resumo executivo da análise de riscos). Para preenchê-la, escreva todos os ativos analisados na Coluna **Ativo**, um em cada linha.

Uma vez elencados todos os ativos anote nas colunas de risco (**Baixo, Médio e Alto**) de cada ativo, os valores de custo e investimento necessários para mitigar, transferir ou controlar os riscos, separando os valores de acordo com a sua intensidade. Estes valores são os mesmos apresentados no modelo da Tabela 17 (Resumo de custos por intensidade do risco) preenchidos durante a análise de cada ativo.

Para os ativos que possuem sistema operacional, deve-se adicionar duas linhas para o ativo, a primeira contendo os valores referentes aos controles específicos para o ativo, e a linha seguinte deve apresentar os custos referentes ao *hardening* do sistema operacional utilizado no ativo. Neste caso, os valores devem ser obtidos das tabelas de *checklist* do ativo e do respectivo *hardening*.

A soma total dos valores de cada linha e de cada coluna deve ser anotada na linha e coluna de totais, respectivamente.

Tabela 19: Exemplo de resumo executivo da análise de riscos

Custos e investimentos estimados necessários para mitigar/controlar os riscos				
Ativo	***Risco***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Firewall Netfilter	1.155	1.050	2.410	4.615
Firewall Netfilter - controles do sistema operacional Linux	245	560	1.120	1.925
Data center	0	7.360	7.800	15.160
Total (R$)				

A separação dos controles de *hardening* dos controles específicos para o ativo, visa facilitar a sua identificação e permitir que sejam implementados em sua totalidade, independente dos itens de controle específicos do ativo. Esta possibilidade é interessante quando, por exemplo, não for possível implementar todos os controles identificados na análise de riscos: neste caso, supondo que a estratégia seja implementar apenas os controles para os riscos de alta intensidade, o processo de *hardening* seria implementado apenas parcialmente se os seus controles fossem tratados juntamente com os demais controles do ativo. Por outro lado, separando-se o *hardening* dos controles específicos do ativo, é possível tratá-lo como um item específico e determinar a sua completa implementação na elaboração da estratégia de implementação dos controles do ativo.

6.7 Recomendações

A metodologia da M2FE recomenda que sejam implementados primeiramente os controles classificados como sendo de alto risco, seguidos pelos controles de médio risco e,

por último, os de baixo risco, desde que o custo de implementação do controle não ultrapasse o valor do risco.

Controles cujo custo seja igual ou superior ao risco devem ser avaliados junto à diretoria.

7 ANÁLISE DE RISCO INICIAL

A M2FE até a presente data, nunca havia realizado nenhuma análise de risco de uma forma estruturada e utilizando uma metodologia. Essa etapa foi realizada com o objetivo de identificar os principais riscos a que ela está exposta e identificar os principais controles a serem implementados.

7.1 Identificação dos Ativos Críticos

A Figura 27 apresenta o relacionamento ente os processos, sistemas e os respectivos ativos.

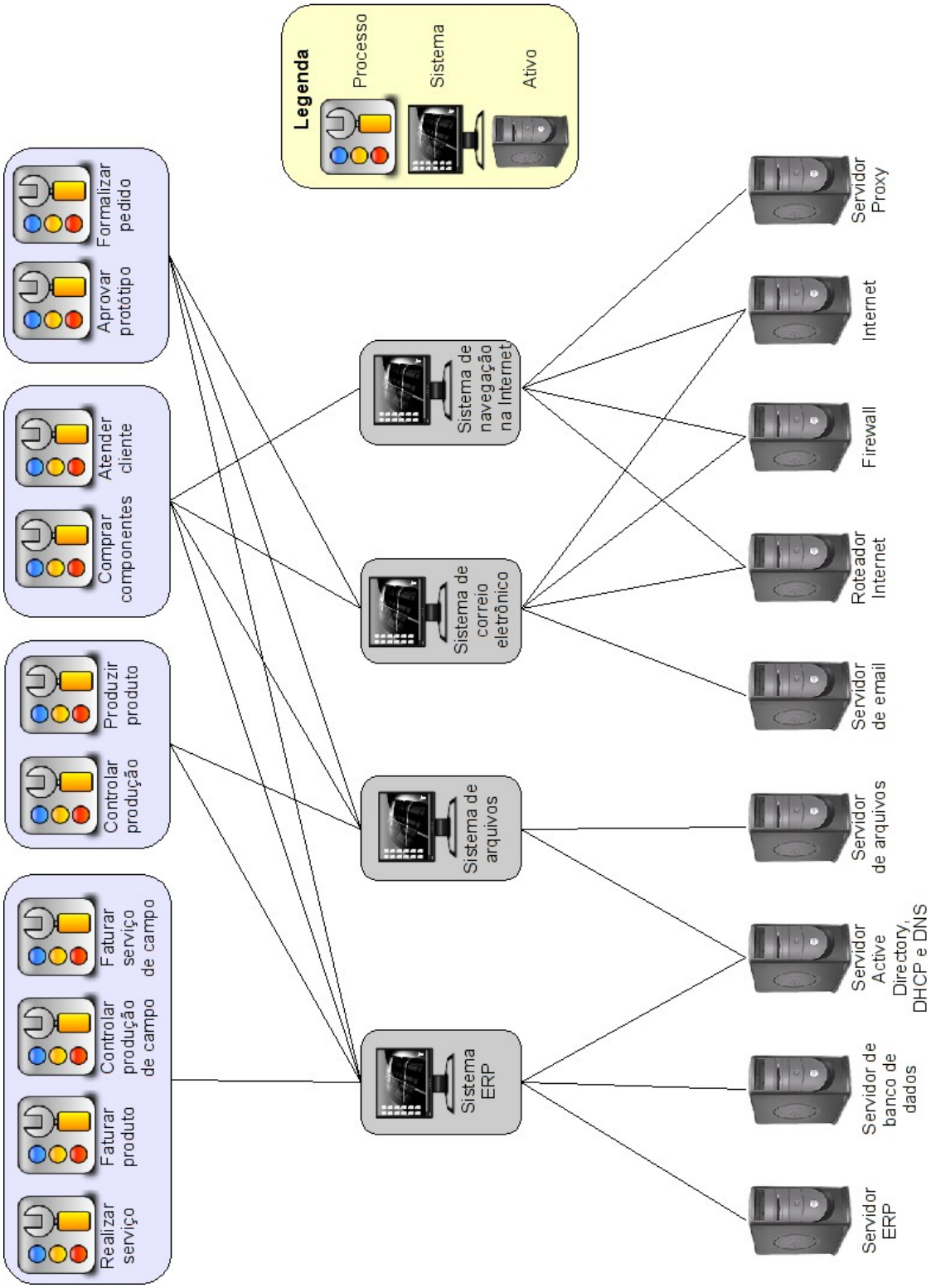


Figura 27: Relacionamento entre processos, sistemas e ativos

Observando o diagrama da Figura 27, mapeamos os relacionamentos entre processos e ativos na Tabela 20 (Relacionamento entre processos e ativos). A partir dessa tabela identificamos os ativos que suportam mais processos.

Tabela 20: Relacionamento entre processos e ativos

	Servidor de arquivos	***Servidor ERP***	***Servidor AD , DHCP e DNS***	***Servidor e-mail***	***Proxy***	***Roteador de Internet***	***Firewall***	***Internet***	***Banco de dados***
Aprovar protótipo	X	X	X	X		X	X		X
Atender cliente	X	X	X	X	X	X	X	X	X
Comprar componentes	X	X	X	X	X	X	X	X	X
Contábil, administrativo e financeiro	X	X	X	X	X	X	X	X	X
Controlar produção	X	X	X						X
Controlar produção de campo		X	X						X
Faturar produto		X	X						X

	Servidor de arquivos	*Servidor ERP*	*Servidor AD , DHCP e DNS*	*Servidor e-mail*	*Proxy*	*Roteador de Internet*	*Firewall*	*Internet*	*Banco de dados*
Faturar serviços de campo		X	X						X
Formalizar pedido	X	X	X	X		X	X	X	X
Produzir produto	X	X	X						X
Realizar serviços		X	X						X

Nem todos os ativos que aparecem nesse mapeamento são críticos, conforme justificativas apresentadas na Tabela 21 (Justificativa de criticidade de ativo).

Tabela 21: Justificativa de criticidade de ativo

Ativo	*Crítico*	*Justificativa*
Servidor de Arquivos	Sim	
Servidor ERP	Sim	
Servidor AD / DHCP / DNS	Sim	
Servidor de *e-mail*	Não	Em contingência as mensagens poderão ser enviadas via fax, correios e outros meios.

Ativo	*Crítico*	*Justificativa*
Servidor *Proxy*	Não	Em contingência os usuários poderão acessar a *Internet* diretamente.
Roteador de *Internet*	Não	Em contingência, todas as transações (pagamento de impostos, pagamentos comerciais, transações financeiras etc) serão realizadas externamente junto às instituições financeiras e os contatos com os clientes e fornecedores serão efetuados via fax e telefone.
Firewall	Sim	
Internet	Não	Em contingência, todas as transações (pagamento de impostos, pagamentos comerciais, transações financeiras etc) serão realizadas externamente junto às instituições financeiras e os contatos com os clientes e fornecedores serão efetuados via fax e telefone.
Servidor de Banco de dados	Sim	
Data center	Sim	Conforme metodologia.
Rede	Sim	Conforme metodologia.
Segurança física	Sim	Conforme metodologia.

7.2 Firewall

O *firewall* utilizado na M2FE consiste num computador padrão IBM-PC que utiliza o sistema operacional *GNU/Linux Debian* 5.0 *(Lenny)* e a filtragem de pacotes é realizada pelo *Netfilter*, que é o filtro de pacotes padrão de sistemas *GNU/Linux*.

7.2.1 Riscos e controles

Os resultados da aplicação do *checklist* de controles é apresentado na Tabela 22 (*Firewall Netfilter* - controles).

Tabela 22: *Firewall Netfilter* - controles

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Versão do *Netfilter* deve ser a versão estável mais atual.	2	TEC	N	1,00	0,00	M	A	A
2	Os registros de *log* do *Netfilter* devem ser analisados diariamente.	1	TEC	N	1,00	0,00	M	M	M
3	Os arquivos de *log* devem ser rotacionados semanalmente.	2	TEC	N	4,00	0,00	M	M	M
4	O *backup* das regras do *Netfilter* deve ser realizado semanalmente.	2	TEC	S	0,00	0,00	B	M	-
5	As regras de filtragem devem ser criadas na ordem correta (e testadas).	8	TEC	N	8,00	0,00	B	A	M

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	O endereço MAC do *gateway* da rede deve ser uma entrada estática na tabela ARP.	8	TEC	N	0,50	0,00	M	B	B
7	Todas as regras do *Netfilter* devem usar endereços IP e não nomes.	8	TEC	S	0,00	0,00	B	M	-
8	As regras antigas devem ser removidas no início da ativação do *Netfilter*.	8	TEC	S	0,00	0,00	B	M	-
9	A filtragem de pacotes por estado (SPF) deve ser utilizada nas regras do *Netfilter*.	8	TEC	S	0,00	0,00	B	M	-
10	O encaminhamento IP (IP Forward) deve ser desabilitado enquanto as regras do *Netfilter* não tiverem sido carregadas.	8	TEC	N	0,50	0,00	M	M	M

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
11	Permitir tráfego de pacotes ICMP apenas para os tipos 0, 3, 8 e 11 (e*cho reply, destination unreachable, echo request* e *time exceeded*).	8	TEC	S	0,00	0,00	B	B	-
12	As regras do *firewall* (*Netfilter*) devem ser revisadas semestralmente.	8	TEC	N	2,00	0,00	M	B	B
13	Apenas tráfego explicitamente autorizado deve ser permitido entre a DMZ e a *intranet*.	1	TEC	N	4,00	0,00	M	A	A
14	Procedimentos de configuração e instalação do *Netfilter* devem estar documentados.	2	TEC	N	8,00	0,00	M	B	B
15	Pacotes com *flags* inválidas devem ser bloqueados.	2	TEC	N	2,00	0,00	B	M	B
16	Pacotes mal formados devem ser bloqueados pelo *Netfilter*.	2	TEC	N	2,00	0,00	M	B	B

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
17	As regras devem impedir a saída de pacotes da rede interna com IPs públicos.	1	TEC	N	1,00	0,00	M	M	M
18	O *firewall Netfilter* deve ser instalado em um computador dedicado.	2	TEC	S	0,00	0,00	B	M	-
19	Ferramentas gráficas de gerenciamento do *Netfilter* devem ser removidas.	1	TEC	S	0,00	0,00	B	M	-
20	As permissões do arquivo de regras devem ser exclusivas ao usuário *root* (0600).	2	TEC	N	0,50	0,00	M	B	B
21	As regras do *Netfilter* devem ser elaboradas de forma a registrar em *log* os eventos do tipo *critical*.	2	TEC	S	0,00	0,00	B	M	-
22	As regras mais utilizadas devem ser posicionadas no início da tabela de regras do *Netfilter*.	2	TEC	N	1,00	0,00	M	B	B

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	O uso da diretiva *any* nas regras do *Netfilter* deve ser evitado ou minimizado.	1	TEC	N	0,50	0,00	M	M	M
24	O conjunto de regras do *Netfilter* deve possuir uma regra que rejeite o tráfego de pacotes do tipo *ident.*	1	TEC	N	0,50	0,00	B	B	B
25	Possui equipamento de reserva?	8	TEC	N	8,00	1500,00	M	A	A

Este ativo utiliza o sistema operacional Linux e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 23 (*Firewall Netfilter:* controles do sistema operacional).

Tabela 23: *Firewall Netfilter*: controles do sistema operacional

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Instalar as correções de segurança sempre que disponibilizadas pelo fabricante.	9	TEC	N	5,00	0,00	A	A	A

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
2	Desabilitar os privilégios SUID e SGID dos programas não essenciais à função do servidor.	9	TEC	N	3,00	0,00	A	A	A
3	Desabilitar o serviço *portmap* se o servidor não utilizar NFS.	9	TEC	N	0,50	0,00	M	A	A
4	Limitar o número de processos que um usuário pode executar simultaneamente.	9	TEC	N	0,50	0,00	M	A	A
5	Remover os serviços não necessários para a função do servidor (FTP, DNS, Apache etc).	9	TEC	N	1,50	0,00	M	A	A
6	Desabilitar o acesso da conta root nos consoles locais.	9	TEC	N	0,50	0,00	B	A	M
7	Criar contas com privilégios mínimos para os administradores e adicioná-las no grupo *wheel.*	9	TEC	N	1,00	0,00	M	A	A

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
8	Permitir a elevação de privilégios através do comando su somente ao grupo *wheel.*	9	TEC	N	0,50	0,00	M	A	A
9	Forçar o serviço SSH a aceitar conexões usando apenas a versão 2 do protocolo.	9	TEC	N	0,50	0,00	M	A	A
10	Adicionar apenas as contas dos administradores no grupo *wheel.*	9	TEC	N	0,50	0,00	M	A	A
11	Desabilitar o acesso da conta *root* via SSH.	9	TEC	N	0,50	0,00	M	A	A
12	Remover *banners* de identificação dos serviços habilitados.	9	TEC	N	1,00	0,00	M	M	M
13	Habilitar o registro de acessos de usuários (arquivos *wtmp* e *btmp*).	9	TEC	N	0,50	0,00	B	B	B
14	Habilitar *log* do sistema, separando por tipo de serviço.	9	TEC	N	0,50	0,00	B	B	B

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
15	Habilitar o uso do PAM (*Pluggable Authentication Modules*).	9	TEC	N	0,50	0,00	M	M	M
16	Habilitar o *flag* tcp_*syncookies* no TCP/IP para combater ataques do tipo *synflood.*	9	TEC	N	0,50	0,00	M	A	A
17	Desabilitar a resposta a requisições ICMP em *broadcast* (ignore_*broadcasts*=1).	9	TEC	N	0,50	0,00	M	M	M
18	Desabilitar o aceite de pacotes IP roteados pela origem (*.accept_source_route=0).	9	TEC	N	0,50	0,00	M	M	M
19	Habilitar a verificação de caminho reverso para combater ataques de IP *spoofing* (*rp_filter=1).	9	TEC	N	0,50	0,00	M	M	M
20	Adicionar as opções de montagem nosuid e noexec nas partições de dados (/home, /var etc).	9	TEC	N	0,50	0,00	M	A	A

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
21	Adicionar as opções de montagem *nosuid*, *noexec*, *nodev* à partição /tmp.	9	TEC	N	0,50	0,00	M	M	M
22	Adicionar as opções de montagem *nodev, noexec* e *nosuid* às mídias removíveis *(fstab)*.	9	TEC	N	0,50	0,00	B	M	B
23	Ajustar o tempo de ociosidade do console para 5 minutos.	9	TEC	N	0,50	0,00	B	B	B
24	O *layout* de particionamento do disco deve ser adequado (/boot, /, /home, /usr, /var, /tmp etc).	9	TEC	N	0,50	0,00	M	A	A
25	Desabilitar desligamento do computador via CTRL+ALT+DEL.	9	TEC	N	0,50	0,00	B	A	M
26	Remover o ambiente gráfico se ele não for estritamente necessário ao funcionamento de alguma aplicação.	9	TEC	N	0,50	0,00	M	A	A

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
27	Habilitar o registro de eventos de uso do sistema (sysstat - comando sar).	9	TEC	N	0,50	0,00	B	M	B
28	Habilitar o *sticky bit* nos diretórios públicos (/tmp por exemplo).	9	TEC	N	0,50	0,00	M	M	M
29	Remover o suporte aos arquivos .rhosts do PAM.	9	TEC	N	0,50	0,00	M	A	A
30	Restringir o acesso ao agendador de tarefas *(cron* e *at)* apenas aos usuários autorizados.	9	TEC	N	0,50	0,00	B	M	B
31	Definir e habilitar senha no gerenciador de inicialização (GRUB/Lilo) para restringir o acesso ao modo monousuário.	9	TEC	N	0,50	0,00	B	A	M
32	Garantir que não haja nenhuma conta de usuário ativa com senha nula.	9	TEC	N	0,50	0,00	M	M	M

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
33	Os diretórios dos usuários (/home) devem possuir atributos 0750 ou mais restritivos.	9	TEC	N	0,50	0,00	M	M	M
34	Ajuste a máscara padrão de criação de arquivos e diretórios para 0770 (não acessíveis globalmente).	9	TEC	N	0,50	0,00	M	M	M
35	Desabilitar a geração de *core dumps* quando programas são abortados.	9	TEC	N	0,50	0,00	B	M	B
36	Desabilitar o *shell* de todas as contas de sistema (serviços).	9	TEC	N	1,00	0,00	M	M	M

7.2.2 Resumo dos riscos

A Tabela 24 (*Firewall Netfilter*: riscos por intensidade) e a Figura 28 resumem a quantidade de riscos a qual o *firewall* está sujeito.

Tabela 24: *Firewall Netfilter*: riscos por intensidade

Firewall *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	18	33,96
M	**Médio**	20	37,74
B	**Baixo**	15	28,30

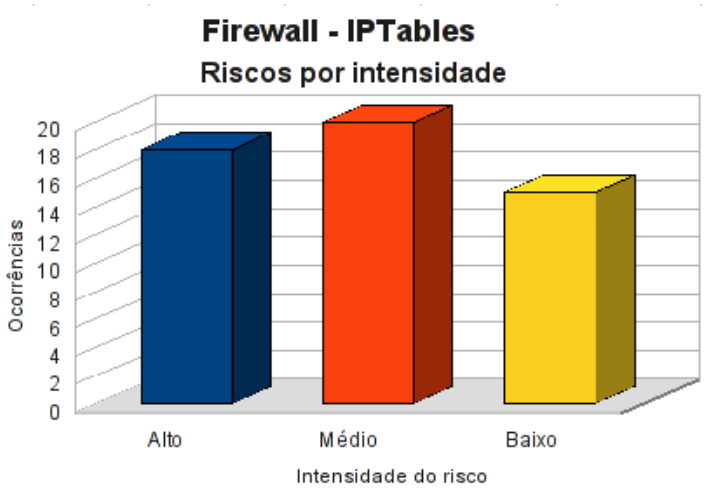


Figura 28: *Firewall Netfilter*: riscos por intensidade

Os riscos identificados para o *firewall* são, na sua totalidade, de características tecnológicas, conforme pode ser observado na Tabela 25 (*Firewall Netfilter:* riscos por tipo de vulnerabilidade) e Figura 29.

Tabela 25: *Firewall Netfilter*: riscos por tipo de vulnerabilidade

Firewall *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	18
M	**Médio**	0	0	20
B	**Baixo**	0	0	15

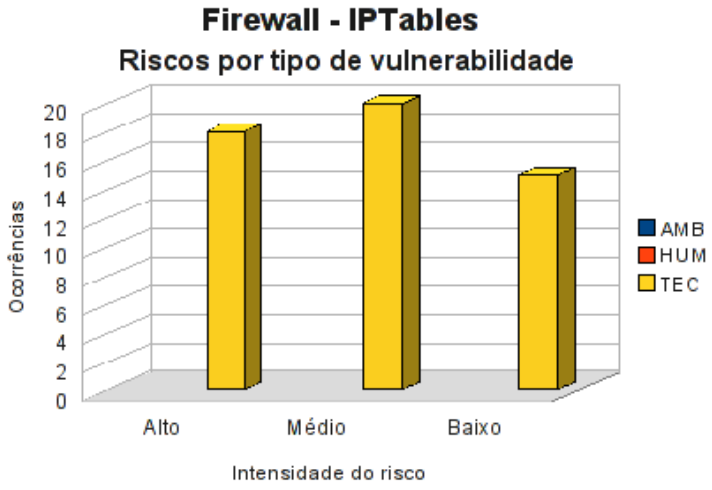


Figura 29: *Firewall Netfilter*: riscos por tipo de vulnerabilidade

7.2.3 Conformidade com os controles

A conformidade com os controles de segurança do *firewall* é apresentada na Tabela 26 (*Firewall Netfilter*: conformidade com os controles) e o gráfico, na Figura 30.

Tabela 26: *Firewall Netfilter*: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	53	86,89
Implementados	8	13,11
Total	**61**	**100,00**

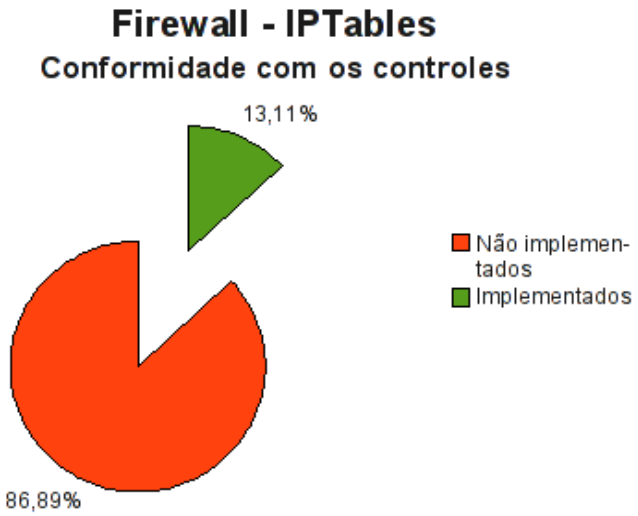


Figura 30: *Firewall Netfilter*: conformidade com os controles

7.2.4 Investimentos necessários

A Tabela 27 (*Firewall Netfilter*: custo estimado para mitigar/controlar os riscos) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *firewall*.

Tabela 27: *Firewall Netfilter*: custo estimado para mitigar/controlar os riscos

Firewall ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	72,00	5040,00
Investimento			1500,00
Total a ser investido			**6540,00**

A Tabela 28 (*Firewall Netfilter:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *firewall,* por intensidade dos riscos.

Tabela 28: *Firewall Netfilter*: custos por intensidade do risco

Firewall ***Custo estimado para mitigar/controlar os riscos*** ***(por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	Alto	3530,00
M	Médio	1610,00
B	Baixo	1400,00
Total		**6540,00**

7.3 Servidor de Banco de Dados

O servidor de banco de dados atualmente utilizado é *Oracle* 9i, sendo executado no ambiente operacional *Windows 2003 Server*.

7.3.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 29 (Servidor de banco de dados: controles).

Tabela 29: Servidor de banco de dados: controles

Servidor de banco de dados		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Versão do *software* deve ser a última disponível e compatível com o sistema.	10	TEC	N	40,00	12000,00	A	A	A
2	Aplicar as correções do banco de dados.	2	TEC	N	40,00	0,00	A	A	A
3	A base de dados de desenvolvimento não deve conter dados de produção.	2	HUM	N	8,00	8000,00	A	A	A
4	O servidor deve ser dedicado.	2	TEC	N	8,00	8000,00	M	M	M

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Usuários padrões de instalação devem ser removidos ou desabilitados.	1	TEC	S	0,00	0,00	A	A	-
6	Senhas criadas durante a instalação (*default*) devem ser substituídas.	1	TEC	N	4,00	0,00	A	A	A
7	As contas dos usuários SYS e SYSTEM devem ser desabilitadas.	1	TEC	S	0,00	0,00	A	A	-
8	Adotar o princípio de privilégio mínimo para as contas de usuários.	1	TEC	S	0,00	0,00	M	M	-
9	Senhas de conexão ao banco de dados devem estar de acordo com a política.	2	TEC	N	2,00	0,00	M	A	A
10	Remover os privilégios do grupo *PUBLIC*.	2	TEC	S	0,00	0,00	A	M	-
11	Restringir a permissão *ANY* somente ao grupo de administradores.	1	TEC	S	0,00	0,00	A	M	-

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Parâmetro *remote_OS_authentication* em *FALSE.*	1	TEC	N	1,00	0,00	B	B	B
13	Parâmetro *remote_login_passwordfile* em *EXCLUSIVE.*	1	TEC	N	1,00	0,00	B	B	B
14	O *Listener* deve exigir autenticação nas conexões.	9	TEC	N	8,00	0,00	A	M	A
15	Acesso físico ao servidor deve ser restrito e controlado.	6	TEC	S	0,00	0,00	A	A	-
16	Desabilitar ou restringir os dispositivos de armazenamento (fita, CD, USB).	1	TEC	N	2,00	0,00	A	A	A
17	A restauração do banco de dados deve ser restrita e autorizada aos administradores.	1	HUM	N	8,00	0,00	A	A	A
18	Dados armazenados em *backup* devem ser cifrados.	1	TEC	N	40,00	10000,00	M	A	A

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
19	O serviço DBSNMP deve estar desabilitado.	2	TEC	S	0,00	0,00	M	M	-
20	Deve haver procedimento para verificar a liberação de novas correções.	10	TEC	N	8,00	0,00	B	B	B
21	O acesso remoto (*Terminal Service*) deve ser restrito e controlados aos administradores.	1	HUM	N	4,00	0,00	A	M	A
22	O tráfego de dados do banco de dados na rede deve ser cifrado.	2	TEC	N	40,00	0,00	A	A	A
23	Não permitir acesso de analistas aos dados de produção.	11	TEC	N	8,00	0,00	A	A	A
24	Bloquear a execução de DDL para o usuário de conexão da aplicação.	2	TEC	S	0,00	0,00	A	A	-
25	Os arquivos de *trace* só devem ser acessíveis pelo DBA.	11	TEC	N	4,00	0,00	A	A	A

Este ativo utiliza o sistema operacional *Windows 2003 Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 30 (Servidor de banco de dados: controles do sistema operacional).

Tabela 30: Servidor de banco de dados: controles do sistema operacional

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	N	2,00	0,00	A	A	A
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	N	2,00	0,00	A	A	A
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	N	4,00	0,00	A	A	A
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Remover todos os compartilhamentos não documentados.	2	TEC	N	1,00	0,00	A	A	A
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	N	6,00	0,00	A	A	A
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	N	2,00	0,00	A	A	A
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	N	1,00	0,00	A	A	A
9	Permitir autenticação somente em NTLMv2.	1	TEC	N	1,00	0,00	A	A	A
10	Garantir que a auditoria esteja habilitada.	1	TEC	N	1,00	0,00	A	A	A
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	N	1,00	0,00	A	A	A

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Desabilitar a conta *guest.*	1	TEC	N	1,00	0,00	A	A	A
13	Renomear a conta do administrador.	1	TEC	N	1,00	0,00	A	A	A
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	N	1,00	0,00	A	A	A
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	N	1,00	0,00	M	M	M
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	N	1,00	0,00	A	A	A
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	N	4,00	0,00	A	A	A

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	N	1,00	0,00	M	M	M
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	N	8,00	0,00	A	A	A
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	N	1,00	0,00	A	A	A
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	N	1,00	0,00	A	A	A
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	N	2,00	0,00	A	A	A

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
23	Garantir que o *backup* siga as especificações da política de *backup*.	2	TEC	N	2,00	0,00	A	A	A
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	N	2,00	0,00	A	A	A
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	N	1,00	0,00	A	A	A
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	N	1,00	0,00	A	A	A
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	N	1,00	0,00	B	B	B

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	N	1,00	0,00	B	B	B
29	Configurar a proteção contra ataques SYN.	9	TEC	N	1,00	0,00	A	A	A
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	N	1,00	0,00	A	A	A
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	N	2,00	0,00	A	A	A
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	N	1,00	0,00	M	M	M
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	N	1,00	0,00	A	A	A
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	N	1,00	0,00	M	M	M

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	N	1,00	0,00	A	A	A
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	N	1,00	0,00	M	B	B
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	N	1,00	0,00	A	A	A
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	N	2,00	0,00	A	A	A
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	N	1,00	0,00	A	A	A

7.3.2 Resumo dos riscos

A Tabela 31 (Servidor de banco de dados: riscos por intensidade) e a Figura 31 apresentam o resumo dos riscos o qual o servidor de banco de dados está sujeito.

Tabela 31: Servidor de banco de dados: riscos por intensidade

Servidor de banco de dados *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	46	80,70
M	**Médio**	5	8,77
B	**Baixo**	6	10,53

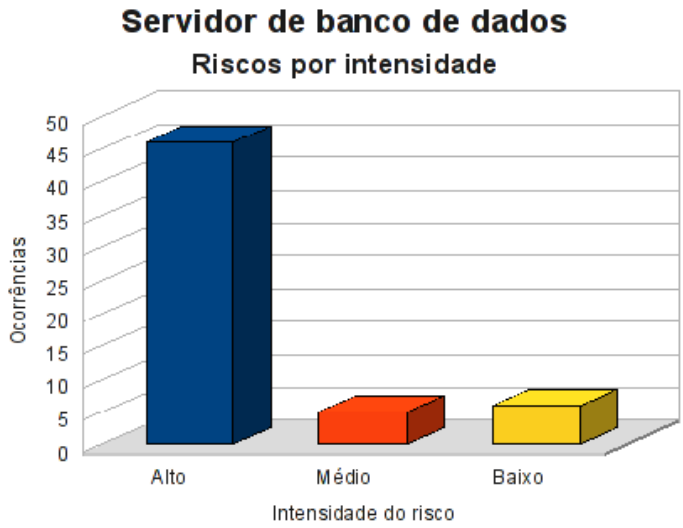


Figura 31: Servidor de banco de dados: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 32 (Servidor de banco de dados: riscos por tipo de vulnerabilidade) e Figura 32.

Tabela 32: Servidor de banco de dados: riscos por tipo de vulnerabilidade

Servidor de banco de dados *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	5	41
M	**Médio**	0	0	5
B	**Baixo**	0	0	6

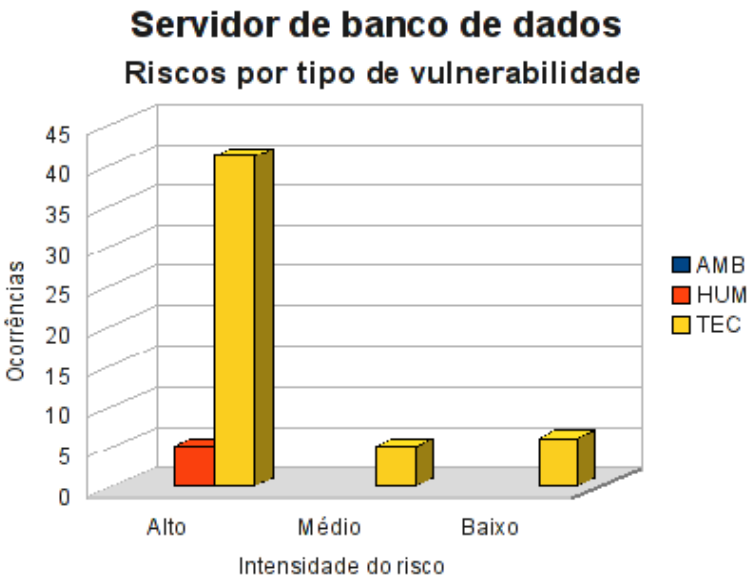


Figura 32: Servidor de banco de dados: riscos por tipo de vulnerabilidade

7.3.3 Conformidade com os controles

A conformidade com os controles de segurança do servidor de banco de dados é apresentada na Tabela 33 (Servidor de banco de dados: conformidade com os controles) e o gráfico na Figura 33.

Tabela 33: Servidor de banco de dados: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	57	87,69
Implementados	8	12,31
Total	**65**	**100**

Figura 33: Servidor de banco de dados: conformidade com os controles

7.3.4 Investimentos necessários

A Tabela 34 (Servidor de banco de dados: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor de banco de dados.

Tabela 34: Servidor de banco de dados: custo estimado para mitigar/controlar os riscos

Servidor de banco de dados *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total***
Custo estimado	70,00	292,00	20440,00
Investimento			38000,00
Total a ser investido			**58440,00**

A Tabela 35 (Servidor de banco de dados*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor de banco de dados por intensidade dos riscos.

Tabela 35: Servidor de banco de dados: custos por intensidade do risco

Servidor de banco de dados *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	48690,00
M	**Médio**	8840,00
B	**Baixo**	910,00
Total		**58440,00**

7.4 Servidor do sistema ERP

O servidor do sistema de ERP da M2FE contém o sistema que permite a manutenção dos dados cadastrais de funcionários e clientes, além dos dados referentes às compras e vendas efetuadas e a geração de relatórios financeiros e estatísticos.

7.4.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 36 (Servidor ERP: controles).

Tabela 36: Servidor ERP: controles

Servidor ERP		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O banco de dados do ERP não pode ser compartilhado com outras aplicações.	2	HUM	N	32,00	8000,00	M	A	A
2	As senhas não devem ser armazenadas pelo sistema, apenas o *hash* das mesmas.	2	TEC	N	16,00	0,00	A	A	A
3	Todos os arquivos da aplicação ou criados pela mesma devem estar protegidos de acessos não autorizados.	2	TEC	N	80,00	0,00	A	M	A

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	As mudanças devem ser analisadas e aprovadas antes da sua implementação.	11	HUM	S	0,00	0,00	A	A	-
5	Documentar os controles de segurança, responsabilidades e procedimentos.	11	HUM	N	240,00	0,00	M	M	M
6	O controle de acesso da aplicação deve ser baseado em segregação de funções.	2	TEC	N	24,00	0,00	M	A	A
7	Somente os responsáveis pela segurança poderão liberar acesso aos usuários.	11	HUM	S	0,00	0,00	M	M	-
8	O acesso à informação, bens e recursos devem ser restritos somente aos usuários autorizados.	2	TEC	S	0,00	0,00	M	M	-
9	As contas de usuários inativos devem ser desabilitadas.	2	TEC	N	16,00	0,00	M	B	B

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	Os procedimentos de atualização de *software* devem estar documentados.	11	HUM	N	24,00	0,00	B	B	B
11	Garantir que os desenvolvedores não tenham acesso ao ambiente de produção.	11	TEC	N	8,00	8000,00	B	A	M
12	Todas as ações dos usuários devem ser registradas em *log* (trilha de auditoria).	1	TEC	N	8,00	0,00	B	M	B
13	As contas de usuários devem ser desativadas após 3 tentativas consecutivas de acesso sem sucesso.	1	TEC	N	8,00	0,00	A	A	A
14	Adotar o princípio de privilégio mínimo para as contas de usuário.	1	TEC	S	0,00	0,00	M	M	-
15	A comunicação entre a aplicação e o banco de dados deve ser cifrada.	2	TEC	N	40,00	0,00	M	A	A

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
16	O código da aplicação não deve ser mantido junto com a aplicação.	11	HUM	N	8,00	0,00	A	A	A
17	Os recursos de rede (IP, URL etc), chaves e senhas não podem ser *hardcoded.*	11	HUM	S	0,00	0,00	A	A	-
18	Os arquivos de *log* devem ser rotacionados semanalmente.	8	TEC	N	4,00	0,00	M	M	M
19	As atividades dos administradores devem ser registradas em *log* e monitoradas.	8	TEC	N	16,00	0,00	B	A	M
20	Deve ser emitido aviso quando os *logs* estiverem a 80% da capacidade de saturação.	1	TEC	N	8,00	0,00	B	B	B
21	Qualquer ferramenta de auditoria devem ser de uso restrito aos auditores.	2	TEC	S	0,00	0,00	B	M	-

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
22	Verificar semestralmente se os *user IDs* são válidos, aprovados e com segregação de funções (auditoria).	11	HUM	N	16,00	0,00	M	A	A
23	Nenhuma conexão anônima deve ser permitida pela aplicação.	9	TEC	S	0,00	0,00	A	A	-
24	Revisar semestralmente as regras de acesso para garantir que nenhuma regra tenha sido alterada.	11	HUM	N	16,00	0,00	B	M	B

Este ativo utiliza o sistema operacional *Windows* 2003 *Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na tabela Tabela 37 (Servidor ERP: controles do sistema operacional).

Tabela 37: Servidor ERP: controles do sistema operacional

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	N	2,00	0,00	A	A	A
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	N	2,00	0,00	A	A	A
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	N	4,00	0,00	A	A	A
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
5	Remover todos os compartilhamentos não documentados.	2	TEC	N	1,00	0,00	A	A	A

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	N	6,00	0,00	A	A	A
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	N	2,00	0,00	A	A	A
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	N	1,00	0,00	A	A	A
9	Permitir autenticação somente em NTLMv2.	1	TEC	N	1,00	0,00	A	A	A
10	Garantir que a auditoria esteja habilitada.	1	TEC	N	1,00	0,00	A	A	A
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	N	1,00	0,00	A	A	A
12	Desabilitar a conta *guest.*	1	TEC	N	1,00	0,00	A	A	A
13	Renomear a conta do administrador.	1	TEC	N	1,00	0,00	A	A	A

Servidor ERP - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	N	1,00	0,00	A	A	A
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	N	1,00	0,00	M	M	M
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	N	1,00	0,00	A	A	A
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	N	4,00	0,00	A	A	A
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	N	1,00	0,00	M	M	M

Servidor ERP - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	N	8,00	0,00	A	A	A
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	N	1,00	0,00	A	A	A
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	N	1,00	0,00	A	A	A
22	As permissões NTFS para o diretório *%SystemRoot %* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	N	2,00	0,00	A	A	A
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	N	2,00	0,00	A	A	A

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	N	2,00	0,00	A	A	A
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	N	1,00	0,00	A	A	A
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	N	1,00	0,00	A	A	A
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	N	1,00	0,00	B	B	B
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	N	1,00	0,00	B	B	B
29	Configurar a proteção contra ataques SYN.	9	TEC	N	1,00	0,00	A	A	A

Servidor ERP - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	N	1,00	0,00	A	A	A
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	N	2,00	0,00	A	A	A
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	N	1,00	0,00	M	M	M
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	N	1,00	0,00	A	A	A
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	N	1,00	0,00	M	M	M
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	N	1,00	0,00	A	A	A
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	N	1,00	0,00	M	B	B

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	N	1,00	0,00	A	A	A
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	N	2,00	0,00	A	A	A
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	N	1,00	0,00	A	A	A

7.4.2 Resumo dos riscos

A Tabela 38 (Servidor ERP: riscos por intensidade) e a Figura 34 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 38: Servidor ERP: riscos por intensidade

Servidor ERP *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	41	71,93
M	**Médio**	8	14,04
B	**Baixo**	8	14,04

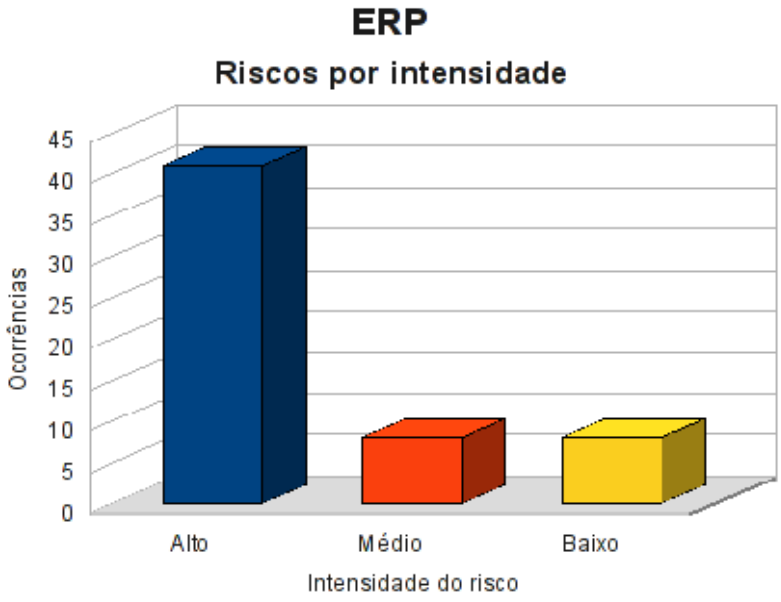


Figura 34: Servidor ERP: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 39 (Servidor ERP: riscos por tipo de vulnerabilidade) e Figura 35.

Tabela 39: Servidor ERP: riscos por tipo de vulnerabilidade

Servidor ERP *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	3	38
M	**Médio**	0	1	7
B	**Baixo**	0	2	6

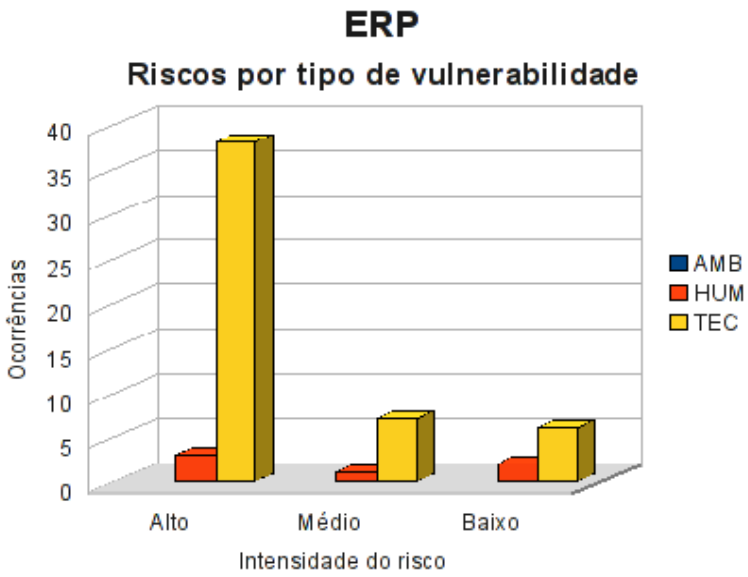


Figura 35: Servidor ERP: riscos por tipo de vulnerabilidade

7.4.3 Conformidade com os controles

A conformidade com os controles de segurança do servidor ERP é apresentada na Tabela 40 (Servidor ERP: conformidade com os controles) e na Figura 36.

Tabela 40: Servidor ERP: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	57	89,06
Implementados	7	10,94
Total	**64**	**100,00**

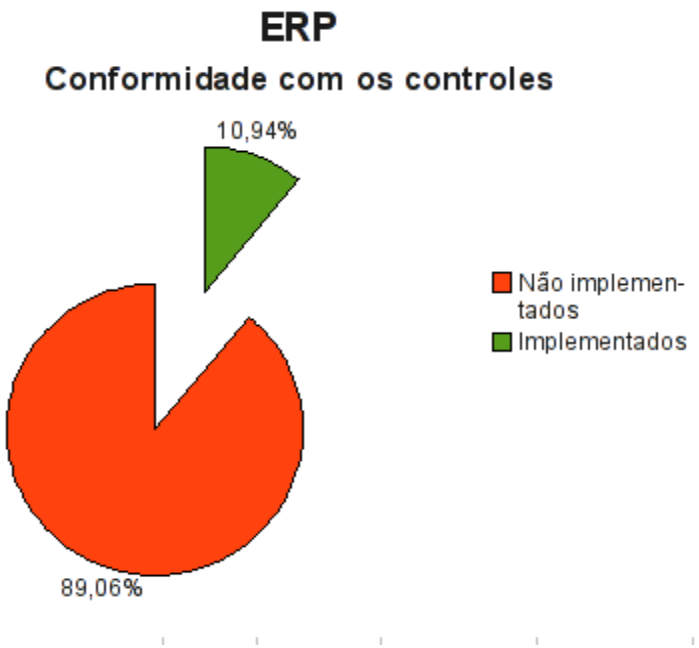


Figura 36: Servidor ERP: conformidade com os controles

7.4.4 Investimentos necessários

A Tabela 41 (Servidor ERP: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor ERP.

Tabela 41: Servidor ERP: custo estimado para mitigar/controlar os riscos

Servidor ERP *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	630,00	44100,00
Investimento			16000,00
Total a ser investido			**60100,00**

A Tabela 42 (Servidor ERP*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor ERP por intensidade dos riscos.

Tabela 42: Servidor ERP: custos por intensidade do risco

Servidor ERP *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	27810,00
M	**Médio**	27040,00
B	**Baixo**	5250,00
Total		**60100,00**

7.5 Servidor Windows Active Directory

O servidor *Windows Active Directory* oferece o serviço de diretório para a rede da M2FE.

Segundo (LOSANO, 2009) "*O serviço de diretório é um conjunto de atributos sobre recursos e serviços existentes na rede, organizando e simplificando o acesso aos recursos da rede centralizando-os, reforçando a segurança e dando proteção aos objetos da base de dados contra intrusos e controlando o acesso dos usuários na rede interna.*".

7.5.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 43 (*Windows Active Directory*: controles).

Tabela 43: *Windows Active Directory*: controles

Windows Active Directory		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Habilitar complexidade de senhas na política de domínio conforme a política da empresa.	1	TEC	S	1,00	0,00	A	A	-
2	Habilitar política de histórico das últimas 5 senhas na política de domínio.	1	TEC	N	1,00	0,00	A	A	A

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
3	Habilitar o requisito mínimo de 8 caracteres para todas as senhas das contas dos domínios.	1	TEC	S	1,00	0,00	A	A	-
4	Habilitar o requisito minimo de 15 caracteres para todas as contas administrativas.	1	TEC	N	1,00	0,00	A	A	A
5	Restringir o acesso remoto aos servidores Controladores de Domínio aos administradores.	1	TEC	N	1,00	0,00	A	A	A
6	Documentar todos servidores *Active Directory* e Global *catalog*.	2	TEC	N	8,00	0,00	A	A	A
7	Documentar o FSMO (regras do domínio).	2	TEC	N	2,00	0,00	A	A	A
8	Garantir que todos os A*ctive Directories* estão sincronizados.	10	TEC	S	8,00	0,00	A	A	-

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
9	Proteger o acesso ao *Active Directory Schema Master* de acesso não autorizado.	1	TEC	S	2,00	0,00	A	A	-
10	Possuir pelo menos 2 servidores controladores de domínio trabalhando ativamente.	10	TEC	N	8,00	5000,00	A	A	A
11	Garantir que os servidores de *Active Directory* são dedicados para esta função.	10	TEC	S	8,00	0,00	A	A	-
12	As contas de serviço devem possuir nomes longos, com alta complexidade de senhas e não podem expirar.	1	TEC	N	2,00	0,00	A	A	A
13	Garantir que os administradores possuem contas separadas para as atividades diárias e outra para as administrativas.	2	TEC	N	1,00	0,00	A	A	A

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	Executar diariamente o *backup* da SAM e do *Schema Master*.	2	TEC	N	1,00	0,00	A	A	A
15	Utilizar o serviço de DNS integrado ao *Active Directory* apenas para *hosts* internos (do domínio).	10	TEC	S	1,00	0,00	A	A	-
16	Possuir ao menos 2 servidores habilitados com *Global Catalog* na Floresta.	10	TEC	N	1,00	0,00	A	A	A
17	Utilizar serviço NTP para sincronização de data e hora para todos os servidores.	10	TEC	N	2,00	0,00	A	A	A
18	Documentar procedimento de promoção e remoção de controladores de domínios.	11	TEC	S	4,00	0,00	A	A	-
19	Garantir que todas as atualizações de segurança sejam instaladas.	1	TEC	N	1,00	0,00	A	A	A

Este ativo utiliza o sistema operacional *Windows* 2003 *Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 44 (*Windows Active Directory*: controles do sistema operacional).

Tabela 44: *Windows Active Directory*: controles do sistema operacional

Windows Active Directory - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	N	2,00	0,00	A	A	A
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	N	2,00	0,00	A	A	A
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	N	4,00	0,00	A	A	A
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Remover todos os compartilhamentos não documentados.	2	TEC	N	1,00	0,00	A	A	A
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	N	6,00	0,00	A	A	A
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	N	2,00	0,00	A	A	A
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	N	1,00	0,00	A	A	A
9	Permitir autenticação somente em NTLMv2.	1	TEC	N	1,00	0,00	A	A	A
10	Garantir que a auditoria esteja habilitada.	1	TEC	N	1,00	0,00	A	A	A
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	N	1,00	0,00	A	A	A

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Desabilitar a conta *guest.*	1	TEC	N	1,00	0,00	A	A	A
13	Renomear a conta do administrador.	1	TEC	N	1,00	0,00	A	A	A
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	N	1,00	0,00	A	A	A
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID.*	2	TEC	N	1,00	0,00	M	M	M
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	N	1,00	0,00	A	A	A
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	N	4,00	0,00	A	A	A

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	N	1,00	0,00	M	M	M
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	N	8,00	0,00	A	A	A
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	N	1,00	0,00	A	A	A
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	N	1,00	0,00	A	A	A
22	As permissões NTFS para o diretório *%SystemRoot %* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	N	2,00	0,00	A	A	A

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	N	2,00	0,00	A	A	A
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	N	2,00	0,00	A	A	A
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	N	1,00	0,00	A	A	A
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	N	1,00	0,00	A	A	A
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	N	1,00	0,00	B	B	B

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	N	1,00	0,00	B	B	B
29	Configurar a proteção contra ataques SYN.	9	TEC	N	1,00	0,00	A	A	A
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	N	1,00	0,00	A	A	A
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	N	2,00	0,00	A	A	A
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	N	1,00	0,00	M	M	M
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	N	1,00	0,00	A	A	A
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	N	1,00	0,00	M	M	M

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	N	1,00	0,00	A	A	A
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	N	1,00	0,00	M	B	B
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	N	1,00	0,00	A	A	A
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
39	Desabilitar a instalação automática de qualquer componente do *Windows.*	2	TEC	N	2,00	0,00	A	A	A
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	N	1,00	0,00	A	A	A

7.5.2 Resumo dos riscos

A Tabela 45 (*Windows Active Directory*: riscos por intensidade) e a Figura 37 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 45: Windows Active Directory: riscos por intensidade

Windows Active Directory ***Resumo dos riscos por intensidade***			
Nível		***Ocorrências***	***%***
A	**Alto**	45	86,54
M	**Médio**	4	7,69
B	**Baixo**	3	5,77

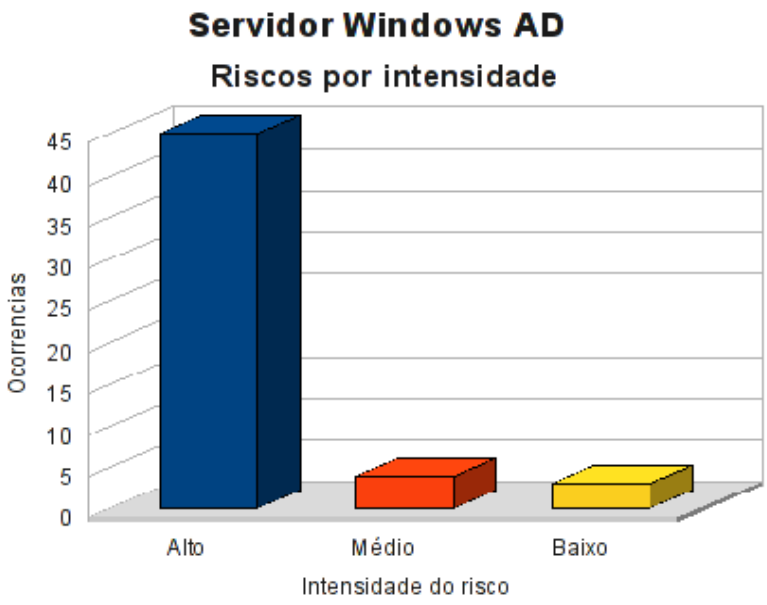


Figura 37: *Windows Active Directory*: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 46 (*Windows Active Directory*: riscos por tipo de vulnerabilidade) e a Figura 38.

Tabela 46: *Windows Active Directory*: riscos por tipo de vulnerabilidade

Windows Active Directory *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	45
M	**Médio**	0	0	4
B	**Baixo**	0	0	3

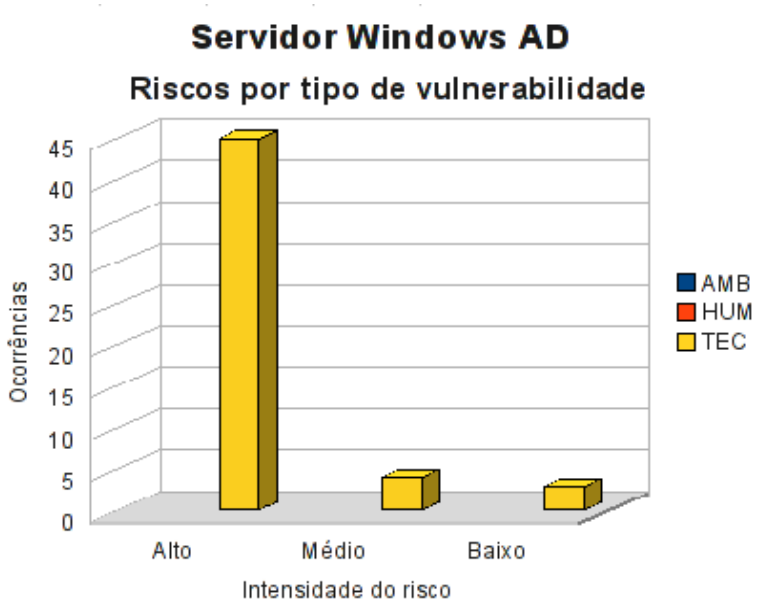


Figura 38: *Windows Active Directory*: riscos por tipo de vulnerabilidade

7.5.3 Conformidade com os controles

A conformidade com os controles de segurança do *Windows Active Directory* é apresentada na Tabela 47 (*Windows Active Directory*: conformidade com os controles) e o gráfico na Figura 39.

Tabela 47: *Windows Active Directory*: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	52	88,14
Implementados	7	11,86
Total	**59**	**100,00**

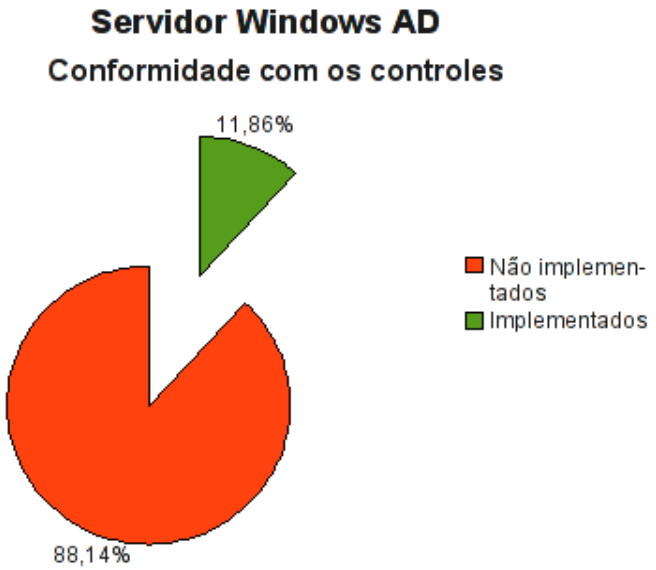


Figura 39: *Windows Active Directory*: conformidade com os controles

7.5.4 Investimentos necessários

A Tabela 48 (*Windows Active Directory*: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Windows Active Directory*.

Tabela 48: *Windows Active Directory*: custo estimado para mitigar/controlar os riscos

Windows Active Directory ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	95,00	6650,00
Investimento			5000,00
Total a ser investido			**11650,00**

A Tabela 49 (*Windows Active Directory:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Windows Active Directory* por intensidade dos riscos.

Tabela 49: *Windows Active Directory*: custos por intensidade do risco

Windows Active Directory ***Custo estimado para mitigar/controlar os riscos*** ***(por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	**Alto**	11160,00
M	**Médio**	280,00
B	**Baixo**	210,00
Total		**11650,00**

7.6 Servidor de arquivos

O servidor de arquivos é o ativo responsável pelo armazenamento e compartilhamento dos arquivos da empresa. Estes arquivos contém, por exemplo, os projetos dos produtos da empresa, planilhas e documentos administrativos.

7.6.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 50 (Servidor de arquivos: controles).

Tabela 50: Servidor de arquivos: controles

Servidor de arquivos		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Todos os compartilhamentos devem ser documentados.	2	TEC	N	8,00	0,00	M	M	M
2	Todos os compartilhamentos devem ser ocultos.	1	TEC	N	2,00	0,00	M	M	M
3	O mapeamento dos compartilhamentos deve ser feito via GPO.	2	TEC	S	0,00	0,00	B	B	-
4	Garantir que o IIS não esteja instalado no servidor.	2	TEC	S	0,00	0,00	A	A	-

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	A estrutura de pastas deve seguir o organograma da empresa.	2	TEC	S	0,00	0,00	A	A	-
6	O diretório *home* de cada usuário deve ter acesso restrito ao usuário proprietário do diretório.	2	TEC	N	8,00	0,00	M	M	M
7	Deve ser configurado uma quota de 1GB por usuário.	10	TEC	S	0,00	0,00	A	A	-
8	O conteúdo do diretório público da rede deve ser apagado diariamente às 00h00.	2	TEC	N	1,00	0,00	M	M	M
9	Documentar todas as unidades mapeadas, conforme sua função.	2	TEC	N	2,00	0,00	A	A	A
10	Deve ser fornecida área cifrada para armazenamento de arquivos classificados como confidenciais.	2	TEC	N	8,00	0,00	A	A	A

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
11	Garantir que o grupo *everyone* (todos) seja removido de todos os compartilhamentos.	2	TEC	N	2,00	0,00	A	A	A
12	Garantir que esteja sendo cumprida a política de *backup.*	2	TEC	N	1,00	0,00	A	A	A
13	Garantir que os arquivos compartilhados estejam em uma partição diferente da utilizada pelo sistema operacional.	2	TEC	S	0,00	0,00	A	A	-
14	Garantir que este servidor seja exclusivo para compartilhamento de arquivos.	10	TEC	S	0,00	0,00	A	A	-
15	Garantir que todos os arquivos de trabalho sejam gravados no servidor.	2	TEC	N	4,00	0,00	A	A	A

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
16	Habilitar o recurso de *Shadow Copies* no volume onde os compartilhamentos estão criados.	2	TEC	N	2,00	0,00	M	M	M
17	Configurar o *Shadow Copies* para executar todos os dias da semana às 10h00 e às 15h00.	2	TEC	N	1,00	0,00	M	M	M
18	Limitar o tamanho do *Shadow copies* para 20GB.	2	TEC	N	1,00	0,00	A	A	A
19	Auditar bimestralmente a conformidade de permissões com as definidas pela diretoria.	2	TEC	N	1,00	0,00	A	A	A

Este ativo utiliza o sistema operacional *Windows* 2003 *Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 51 (Servidor de arquivos: controles do sistema operacional).

Tabela 51: Servidor de arquivos: controles do sistema operacional

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	N	2,00	0,00	A	A	A
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	N	2,00	0,00	A	A	A
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	N	4,00	0,00	A	A	A
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
5	Remover todos os compartilhamentos não documentados.	2	TEC	N	1,00	0,00	A	A	A

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	N	6,00	0,00	A	A	A
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	N	2,00	0,00	A	A	A
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	N	1,00	0,00	A	A	A
9	Permitir autenticação somente em NTLMv2.	1	TEC	N	1,00	0,00	A	A	A
10	Garantir que a auditoria esteja habilitada.	1	TEC	N	1,00	0,00	A	A	A
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	N	1,00	0,00	A	A	A
12	Desabilitar a conta *guest.*	1	TEC	N	1,00	0,00	A	A	A
13	Renomear a conta do administrador.	1	TEC	N	1,00	0,00	A	A	A

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	N	1,00	0,00	A	A	A
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\AppID*.	2	TEC	N	1,00	0,00	M	M	M
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	N	1,00	0,00	A	A	A
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	N	4,00	0,00	A	A	A
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	N	1,00	0,00	M	M	M

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	N	8,00	0,00	A	A	A
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	N	1,00	0,00	A	A	A
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	N	1,00	0,00	A	A	A
22	As permissões NTFS para o diretório *%SystemRoot %* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	N	2,00	0,00	A	A	A
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	N	2,00	0,00	A	A	A

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	N	2,00	0,00	A	A	A
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	N	1,00	0,00	A	A	A
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	N	1,00	0,00	A	A	A
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	N	1,00	0,00	B	B	B
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	N	1,00	0,00	B	B	B

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
29	Configurar a proteção contra ataques SYN.	9	TEC	N	1,00	0,00	A	A	A
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	N	1,00	0,00	A	A	A
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	N	2,00	0,00	A	A	A
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	N	1,00	0,00	M	M	M
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	N	1,00	0,00	A	A	A
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	N	1,00	0,00	M	M	M
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	N	1,00	0,00	A	A	A

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	N	1,00	0,00	M	B	B
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	N	1,00	0,00	A	A	A
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	N	1,00	0,00	A	A	A
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	N	2,00	0,00	A	A	A
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	N	1,00	0,00	A	A	A

7.6.2 Resumo dos riscos

A Tabela 52 (Servidor de arquivos: riscos por intensidade) e a Figura 40 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 52: Servidor de arquivos: riscos por intensidade

Servidor de arquivos *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	40	75,47
M	**Médio**	10	18,87
B	**Baixo**	3	5,66

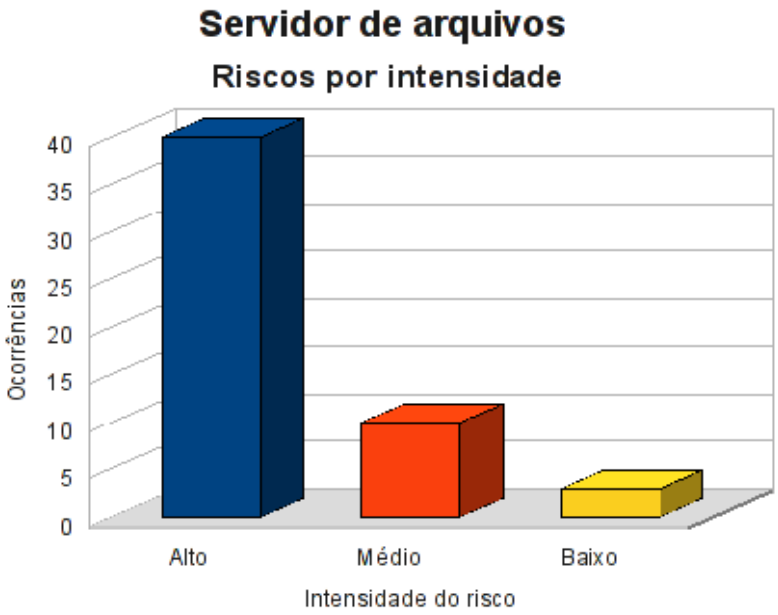


Figura 40: Servidor de arquivos: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 53 (Servidor de arquivos: riscos por tipo de vulnerabilidade) e a Figura 41.

Tabela 53: Servidor de arquivos: riscos por tipo de vulnerabilidade

Servidor de arquivos *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	40
M	**Médio**	0	0	10
B	**Baixo**	0	0	3

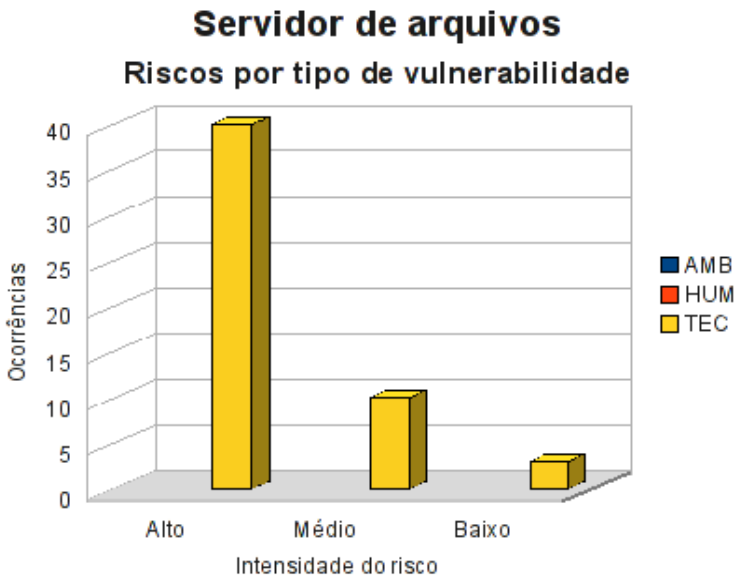


Figura 41: Servidor de arquivos: riscos por tipo de vulnerabilidade

7.6.3 Conformidade com os controles

A conformidade com os controles de segurança do Servidor de arquivos é apresentada na Tabela 54 (Servidor de arquivos: conformidade com os controles) e o gráfico, na Figura 42.

Tabela 54: Servidor de arquivos: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	53	89,83
Implementados	6	10,17
Total	**59**	**100,00**

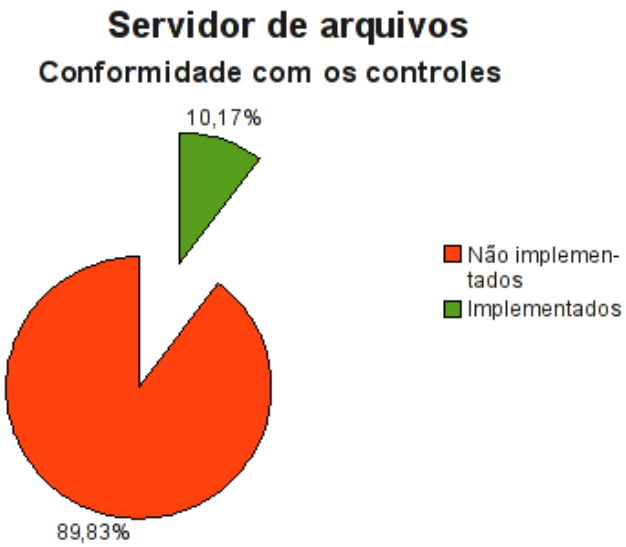


Figura 42: Servidor de arquivos: conformidade com os controles

7.6.4 Investimentos necessários

A Tabela 55 (Servidor de arquivos: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no Servidor de arquivos.

Tabela 55: Servidor de arquivos: custo estimado para mitigar/controlar os riscos

Servidor de arquivos *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	107,00	7490,00
Investimento			0,00
Total a ser investido			**7490,00**

A Tabela 56 (Servidor de arquivos*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no Servidor de arquivos por intensidade dos riscos.

Tabela 56: Servidor de arquivos: custos por intensidade do risco

Servidor de arquivos *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	5460,00
M	**Médio**	1820,00
B	**Baixo**	210,00
Total		**7490,00**

7.7 Data center

O *Data center* é o local onde a maioria dos servidores e equipamentos de rede são alojados.

7.7.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 57 (*Data center*: controles).

Tabela 57: *Data center*: controles

Data center		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Remover do interior do *data center* todos os materiais não relacionados às atividades do mesmo.	11	HUM	N	8,00	0,00	M	M	M
2	Instalar filtros de limpeza ou contra gases e vapores.	7	TEC	N	16,00	1000,00	M	M	M
3	Deve existir um termostato exclusivo para controle de temperatura do *data center*.	10	TEC	S	0,00	0,00	M	M	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	Deve ser definido e instalado um sistema de refrigeração de contingência para o *data center*.	4	TEC	N	40,00	5000,00	A	A	A
5	O sistema de refrigeração do *data center* deve ser exclusivo.	4	TEC	S	0,00	0,00	M	M	-
6	Devem ser elaborados registros de manutenção preventiva do sistema de ar condicionado.	4	TEC	S	0,00	0,00	A	M	-
7	Instalar câmeras de CFTV externas e internas ao *data center* e armazenar as imagens por 180 dias.	1	TEC	N	16,00	1000,00	M	M	M
8	Não permitir o acesso de visitantes ao *data center* sem prévia autorização da segurança e sem acompanhante.	1	HUM	S	0,00	0,00	A	A	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
9	A porta do *data center* deve ser provida de mecanismo de fechamento automático.	1	TEC	N	8,00	2000,00	M	M	M
10	Os circuitos elétricos do *data center* devem ser divididos e dimensionados adequadamente.	10	TEC	S	0,00	0,00	A	A	-
11	Devem ser instalados circuitos elétricos com tomadas suficientes para o *data center*.	8	TEC	S	0,00	0,00	A	M	-
12	Devem ser instaladas pelo menos duas unidades de luz de emergência no interior do *data center*.	8	TEC	S	0,00	0,00	M	B	-
13	A tensão de alimentação dos equipamentos do *data center* deve ser estabilizada.	8	TEC	S	0,00	0,00	A	M	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	Devem ser instalados *no-breaks* para os equipamentos críticos do *data center.*	8	TEC	S	0,00	0,00	A	A	-
15	Não deve haver nenhuma identificação da localização do *data center.*	1	HUM	S	0,00	0,00	B	B	-

7.7.2 Resumo dos riscos

A Tabela 58 (*Data center*: riscos por intensidade) e a Figura 43 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 58: *Data center*: riscos por intensidade

Data center *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	1	20,00
M	**Médio**	4	80,00
B	**Baixo**	0	0,00

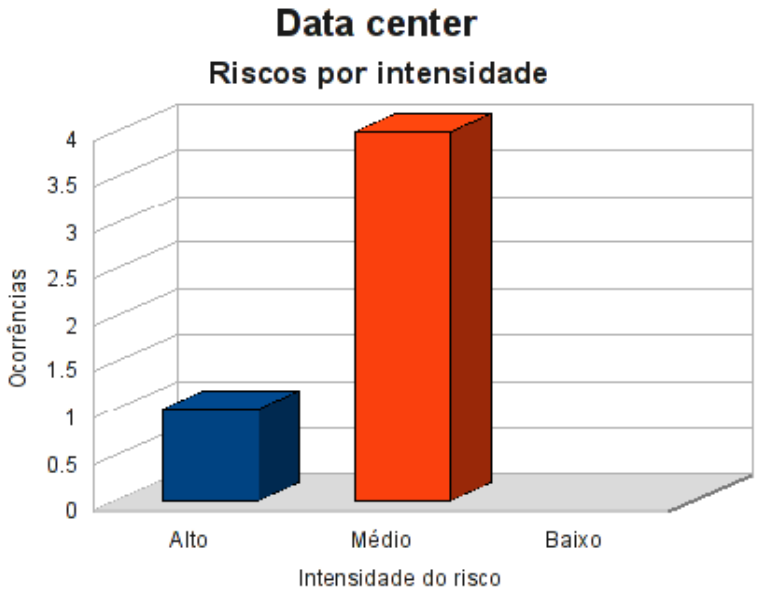


Figura 43: *Data center*: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 59 (*Data center*: riscos por tipo de vulnerabilidade) e na Figura 44.

Tabela 59: *Data center*: riscos por tipo de vulnerabilidade

Data center ***Resumo dos riscos por tipo de vulnerabilidade***				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	1
M	**Médio**	0	1	3
B	**Baixo**	0	0	0

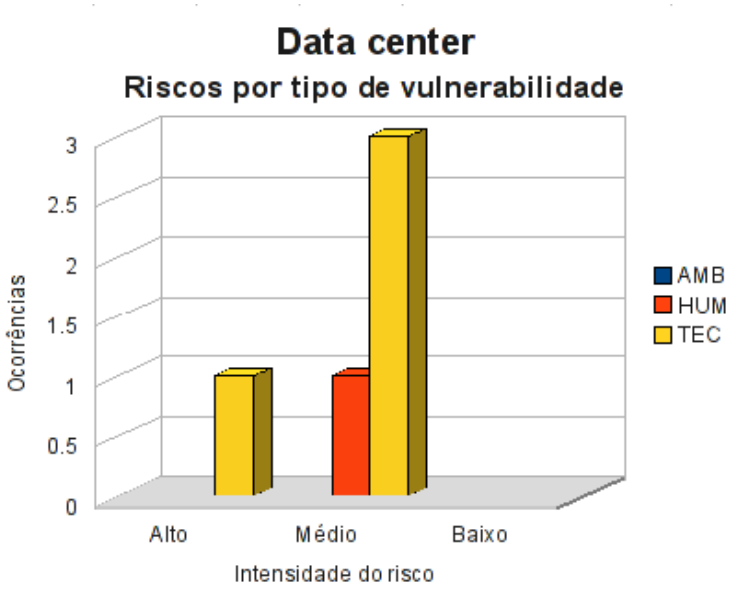


Figura 44: *Data center*: riscos por tipo de vulnerabilidade

7.7.3 Conformidade com os controles

A conformidade com os controles de segurança do *Data center* é apresentada na Tabela 60 (*Data center*: conformidade com os controles) e o gráfico, na Figura 45.

Tabela 60: Data center: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	5	33,33
Implementados	10	66,67
Total	**15**	**100,00**

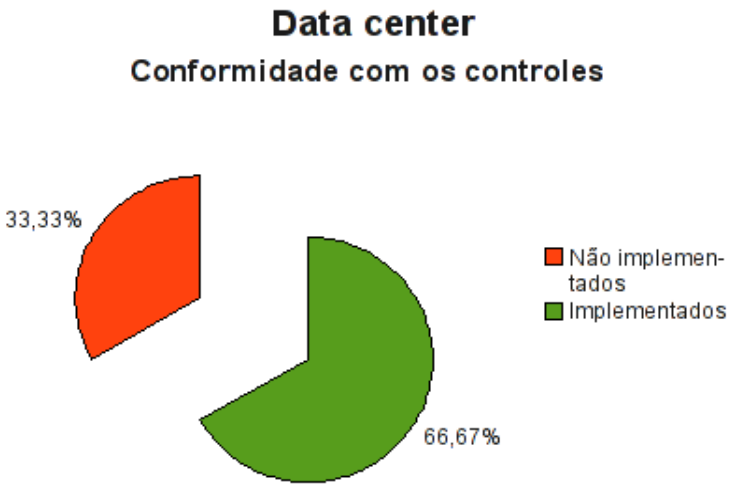


Figura 45: *Data center*: conformidade com os controles

7.7.4 Investimentos necessários

A Tabela 61 (*Data center*: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *data center*.

Tabela 61: *Data center*: custo estimado para mitigar/controlar os riscos

Data center ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	88,00	6160,00
Investimento			9000,00
Total a ser investido			**15160,00**

A Tabela 62 (*Data center:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Data center* por intensidade dos riscos.

Tabela 62: Data center: custos por intensidade do risco

Data center ***Custo estimado para mitigar/controlar os riscos (por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	**Alto**	7800,00
M	**Médio**	7360,00
B	**Baixo**	0,00
Total		**15160,00**

7.8 Análise da rede

Na análise de riscos da rede, a preocupação recai sobre as características específicas da rede da M2FE.

7.8.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 63 (Rede: controles).

Tabela 63: Rede: controles

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O endereçamento IP utilizado na LAN é privado (RFC1918).	8	TEC	S	0,00	0,00	B	B	-
2	O cabeamento de rede é certificado.	8	TEC	S	0,00	0,00	B	B	-
3	Devem ser utilizadas fibras ópticas com redundância entre os *switches* de distribuição e o *Core.*	8	TEC	S	0,00	0,00	B	B	-
4	A topologia da rede deve ser estruturada em formato *full mesh* (redundância).	8	TEC	N	8,00	2000,00	B	M	B
5	O protocolo STP deve estar habilitado e configurado corretamente.	8	TEC	N	4,00	0,00	B	M	B
6	A rede deve ser segmentada.	8	TEC	N	80,00	0,00	M	A	A

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
7	Deve ser utilizado *switch core* L3 com redundância.	8	TEC	N	8,00	10000,00	B	A	M
8	Devem ser Implementadas *Access Control List*s entre VLANs.	8	TEC	N	40,00	0,00	M	A	A
9	Deve haver *firewall* entre as VLANs.	8	TEC	N	80,00	15000,00	M	M	M
10	Deve haver IPS em todos os segmentos da LANs.	8	TEC	N	80,00	15000,00	M	M	M
11	NAC está implementado	8	TEC	N	80,00	15000,00	M	M	M
12	Utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory.*	8	TEC	N	80,00	10000,00	M	M	M
13	Deve ser utilizado protocolo de roteamento autenticado.	8	TEC	N	8,00	0,00	B	B	B

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	Deve haver sumarização de rotas.	8	TEC	N	40,00	0,00	B	B	B
15	Os *links* de dados através da WAN devem ser cifrados.	8	TEC	N	16,00	15000,00	B	B	B
16	Deve haver *switches* de reserva.	10	TEC	N	4,00	2000,00	B	B	B
17	Os *racks* de distribuição devem possuir ventilação adequada.	8	TEC	S	0,00	0,00	B	M	-
18	Os cabeamentos estruturados devem ser separados dos cabeamentos elétricos	8	TEC	S	0,00	0,00	B	B	-
19	A função *anti-snooping* deve ser habilitada nos *switches*.	8	TEC	N	4,00	0,00	B	A	M
20	O servidor DNS deve estar configurado conforme orientação do fabricante.	8	TEC	S	0,00	0,00	M	A	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
21	O parâmetro de atualização dinâmica de zona deve estar habilitado no servidor (Windows).	8	TEC	S	0,00	0,00	M	A	-
22	O DNS deve estar integrado ao *Active Directory*.	8	TEC	S	0,00	0,00	M	A	-
23	O IPSEC deve estar configurado na comunicação entre o ERP e o banco de dados.	8	TEC	N	16,00	0,00	B	M	B
24	Deve ser desativada a *community public* do SNMP.	8	TEC	N	8,00	0,00	B	B	B
25	A rede sem fio não deve propagar o SSID.	8	TEC	S	0,00	0,00	B	B	-
26	O filtro de endereços MAC deve estar habilitado na rede sem fio.	8	TEC	S	0,00	0,00	B	B	-
27	A criptografia da rede sem fio deve estar no modo WPA2.	8	TEC	S	0,00	0,00	B	M	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Todo dispositivo sem fio deve utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory*.	8	TEC	N	8,00	0,00	B	M	B
29	Os *firmwares* de todos os ativos de rede devem estar atualizados para a última versão.	8	TEC	N	40,00	0,00	B	M	B
30	O sinal da rede sem fio não deve propagar além do perímetro físico da empresa.	8	TEC	S	0,00	0,00	B	A	-
31	A conexão com dispositivos de rede sem fio deve ser desativada após 15 minutos sem uso.	8	TEC	N	8,00	0,00	B	B	B
32	Todos os ativos de rede devem ter as senhas padrão alteradas.	8	TEC	N	8,00	0,00	M	M	M

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
33	Garantir que o ponto de acesso está em local seguro.	4	TEC	S	0,00	0,00	B	B	-
34	Serviços acessíveis externamente devem estar na DMZ.	8	TEC	N	40,00	2000,00	A	A	A
35	O *Port Security* deve estar habilitado nos *switches*.	8	TEC	N	40,00	0,00	M	M	M
36	Deve haver um servidor de DHCP *backup* para distribuição de endereçamento IP.	8	TEC	N	6,00	0,00	B	B	B
37	Garantir que não existam *links* externos não gerenciados.	8	TEC	N	20,00	0,00	M	M	M

7.8.2 Resumo dos riscos

A Tabela 64 (Rede: riscos por intensidade) e a Figura 46 apresentam o resumo dos riscos aos quais a rede está sujeita.

Tabela 64: Rede: riscos por intensidade

Rede *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	3	12,50
M	**Médio**	9	37,50
B	**Baixo**	12	50,00

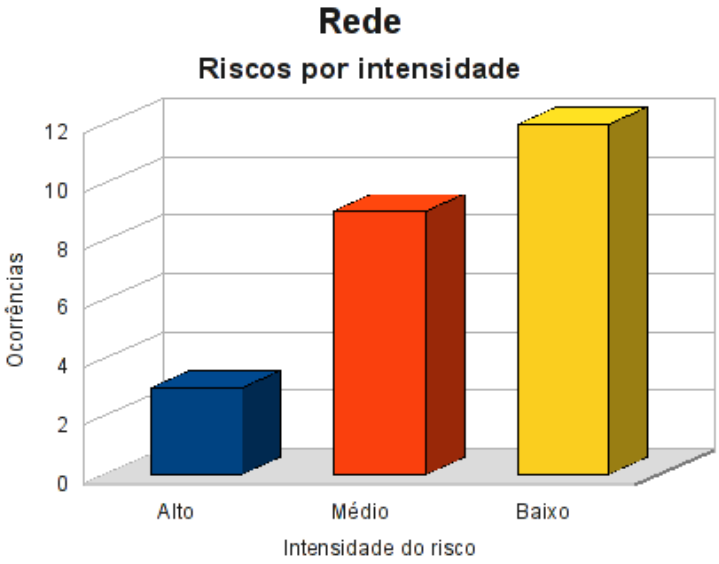


Figura 46: Rede: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 65 (Rede: riscos por tipo de vulnerabilidade) e a Figura 47.

Tabela 65: Rede: riscos por tipo de vulnerabilidade

Rede *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	3
M	**Médio**	0	0	9
B	**Baixo**	0	0	12

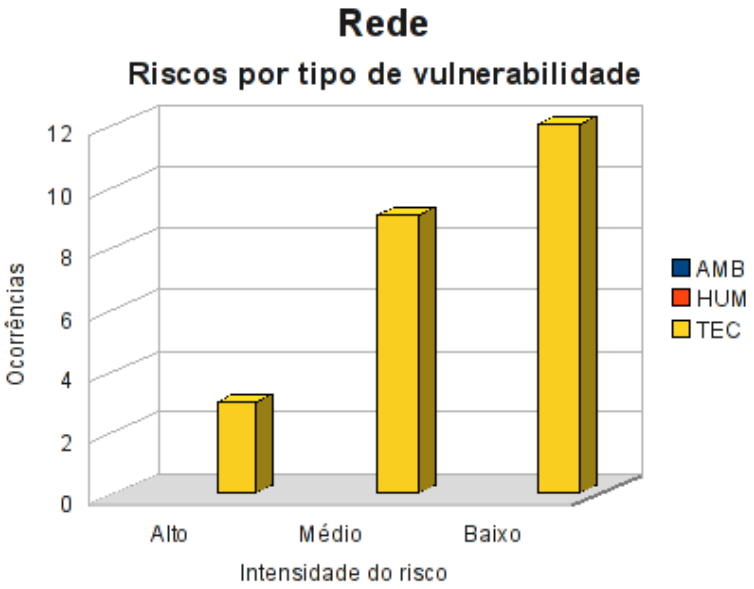


Figura 47: Rede: riscos por tipo de vulnerabilidade

7.8.3 Conformidade com os controles

A conformidade com os controles de segurança da rede é apresentada na Tabela 66 (Rede: conformidade com os controles) e o gráfico, na Figura 48.

Tabela 66: Rede: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	24	64,86
Implementados	13	35,14
Total	**37**	**100,00**

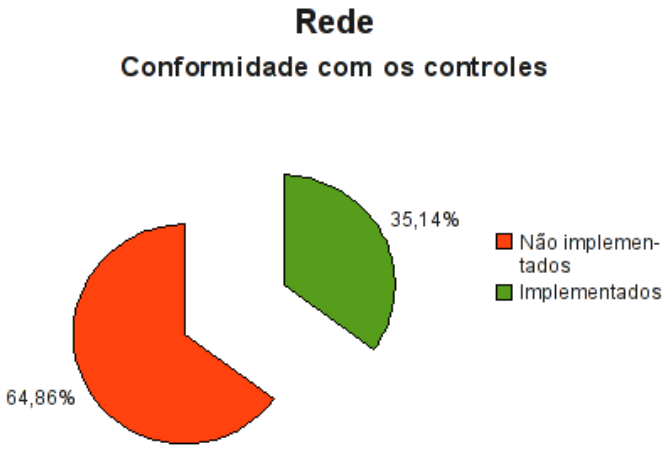


Figura 48: Rede: conformidade com os controles

7.8.4 Investimentos necessários

A Tabela 67 (Rede: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na rede.

Tabela 67: Rede: custo estimado para mitigar/controlar os riscos

Rede *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	726,00	50820,00
Investimento			86000,00
Total a ser investido			**136820,00**

A Tabela 68 (Rede*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na rede por intensidade dos riscos.

Tabela 68: Rede: custos por intensidade do risco

Rede *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	13200,00
M	**Médio**	93000,00
B	**Baixo**	30620,00
Total		**136820,00**

7.9 Segurança física

Na análise de riscos da segurança física a preocupação recai sobre a estrutura física da empresa e as possíveis ameaças a que ela está sujeita.

7.9.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 69 (Segurança física: controles).

Tabela 69: Segurança física: controles

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O perímetro externo da empresa deve ter cerca com altura igual ou superior a 2,5 metros.	1	HUM	S	0,00	0,00	B	B	-
2	Deve haver sensores de invasão no perímetro da empresa.	1	HUM	N	40,00	10000,00	B	B	B
3	Deve haver guarda patrimonial 24 horas por dia.	1	HUM	S	0,00	0,00	A	A	-
4	O perímetro externo da empresa deve possuir placa de aviso de propriedade privada.	1	HUM	S	0,00	0,00	B	B	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Deve haver cães de guarda treinados.	1	HUM	S	0,00	0,00	M	M	-
6	Deve existir sistema de detecção e combate a incêndio.	1	AMB	S	0,00	0,00	B	A	-
7	As áreas criticas devem possuir controle de acesso.	1	TEC	N	8,00	4000,00	M	M	M
8	Devem ser elaborados registros de manutenção preventiva do sistema de alarme.	4	HUM	N	4,00	0,00	B	B	B
9	Deve haver câmeras de CFTV externas e internas e as imagens devem ser retidas por 180 dias.	1	HUM	N	40,00	18000,00	M	M	M
10	A brigada de incêndio deve ser treinada anualmente.	1	HUM	S	0,00	0,00	B	A	-
11	Todos os painéis de distribuição devem ser trancados.	1	HUM	S	0,00	0,00	B	M	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Os circuitos elétricos devem ser divididos e dimensionados adequadamente.	10	TEC	S	0,00	0,00	A	A	-
13	Devem ser instalados pára-raios para a proteção dos equipamentos e do prédio.	7	AMB	S	0,00	0,00	B	A	-
14	Deve haver uma malha de aterramento elétrico para os equipamentos elétricos e eletrônicos.	8	AMB	S	0,00	0,00	M	A	-
15	Todas as eletro-calhas e tubulações metálicas devem ser aterradas.	8	AMB	S	0,00	0,00	M	A	-
16	O grupo moto-gerador deve ser testado mensalmente.	8	TEC	N	4,00	0,00	B	M	B
17	Devem ser instaladas unidades de luz de emergência no interior da empresa.	8	TEC	S	0,00	0,00	B	B	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Todos os circuitos elétricos devem ser protegidos por disjuntores termomagnéticos.	8	TEC	S	0,00	0,00	A	A	-
19	Todos os circuitos elétricos devem ser identificados com etiquetas legíveis.	8	HUM	S	0,00	0,00	B	B	-
20	Deve ser elaborado um mecanismo de registro de incidentes de segurança física.	11	HUM	N	8,00	0,00	B	B	B
21	Todos os visitantes devem ser devidamente identificados, registrados e portar crachá em local visível.	4	AMB	S	0,00	0,00	B	A	-
22	O sistema de alarme de incêndio deve ser testado mensalmente e o teste deve ser registrado.	4	TEC	S	0,00	0,00	B	A	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Os extintores de incêndio devem ser inspecionados trimestralmente (com registro).	4	TEC	S	0,00	0,00	B	A	-
24	O cabeamento deve ser verificado quanto à conformidade com as normas de cabeamento estruturado.	10	TEC	S	0,00	0,00	A	M	-
25	Todos os cabos devem ser devidamente identificados.	10	TEC	S	0,00	0,00	B	B	-
26	Os cabeamentos de dados, telefonia e de energia elétrica devem ser instalados fisicamente separados.	8	TEC	S	0,00	0,00	A	M	-
27	Os cabos de dados do *data center* devem ser instalados diretamente (ponto-a-ponto) sem emendas.	8	TEC	S	0,00	0,00	A	M	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Os dutos de ar condicionado devem ser revestidos externamente por material térmico e não combustível.	4	TEC	S	0,00	0,00	A	A	-
29	Os equipamentos de refrigeração instalados externamente devem ser devidamente protegidos contra acesso físico não autorizado.	1	TEC	S	0,00	0,00	M	A	-
30	Os vidros da guarita de entrada devem ser escuros ou cobertos com película protetora escura.	1	AMB	N	0,00	200,00	M	M	M

7.9.2 Resumo dos riscos

A Tabela 70 (Segurança física: riscos por intensidade) e a Figura 49 apresentam o resumo dos riscos relacionados à segurança física.

Tabela 70: Segurança física: riscos por intensidade

Segurança física *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	3	42,86
B	**Baixo**	4	57,14

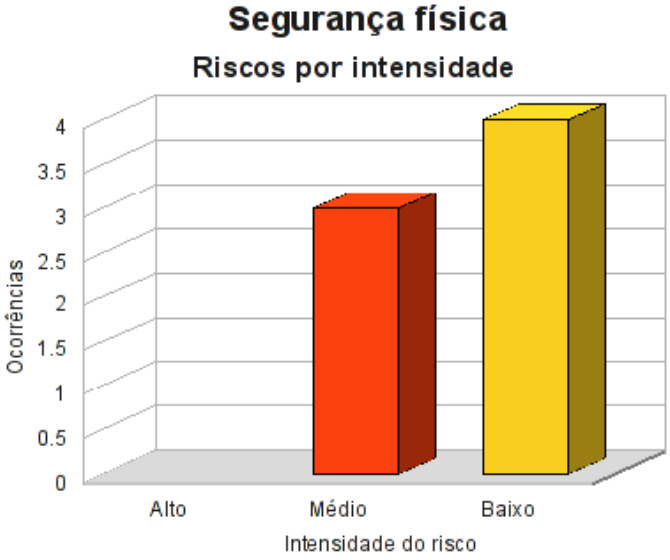


Figura 49: Segurança física: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 71 (Segurança física: riscos por tipo de vulnerabilidade) e a Figura 50.

Tabela 71: Segurança física: riscos por tipo de vulnerabilidade

Segurança física *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	1	1	1
B	**Baixo**	0	3	1

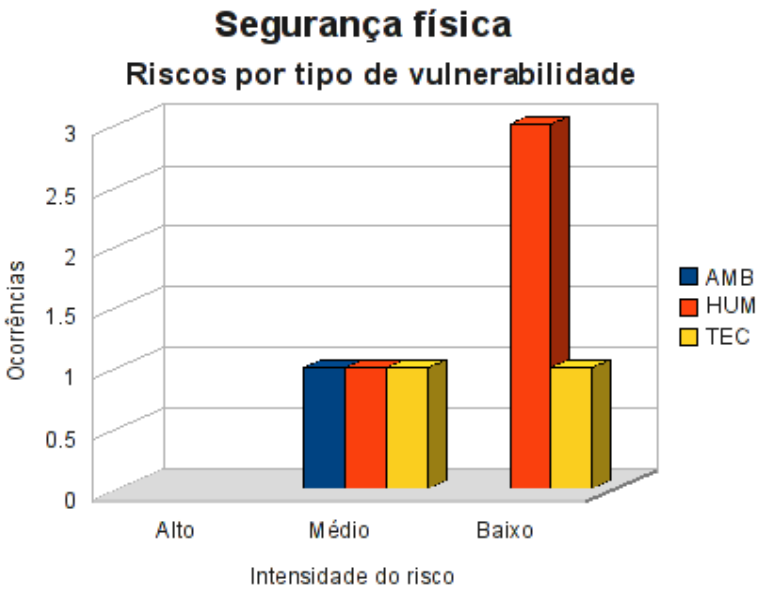


Figura 50: Segurança física: riscos por tipo de vulnerabilidade

7.9.3 Conformidade com os controles

A conformidade com os controles de segurança física é apresentada na Tabela 72 (Segurança física: conformidade com os controles) e o gráfico, na Figura 51.

Tabela 72: Segurança física: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	7	23,33
Implementados	23	76,67
Total	**30**	**100,00**

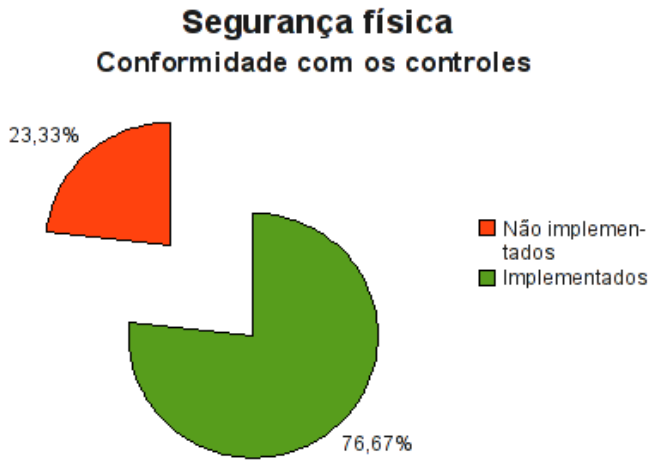


Figura 51: Segurança física: conformidade com os controles

7.9.4 Investimentos necessários

A Tabela 73 (Segurança física: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na segurança física.

Tabela 73: Segurança física: custo estimado para mitigar/controlar os riscos

Segurança física *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	104,00	7280,00
Investimento			32200,00
Total a ser investido			**39480,00**

A Tabela 74 (Segurança física*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na segurança física por intensidade dos riscos.

Tabela 74: Segurança física: custos por intensidade do risco

Segurança física *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	25560,00
B	**Baixo**	13920,00
Total		**39480,00**

7.10 Resumo executivo

Os ativos da M2FE não estão totalmente em conformidade com os controles de segurança, como pode ser observado na Tabela 75 (Resumo geral de conformidade com os controles) e representado no gráfico, da Figura 52.

Tabela 75: Resumo geral de conformidade com os controles

Resumo geral de conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	308	78,97
Implementados	82	21,03
Total	**390**	**100,00**

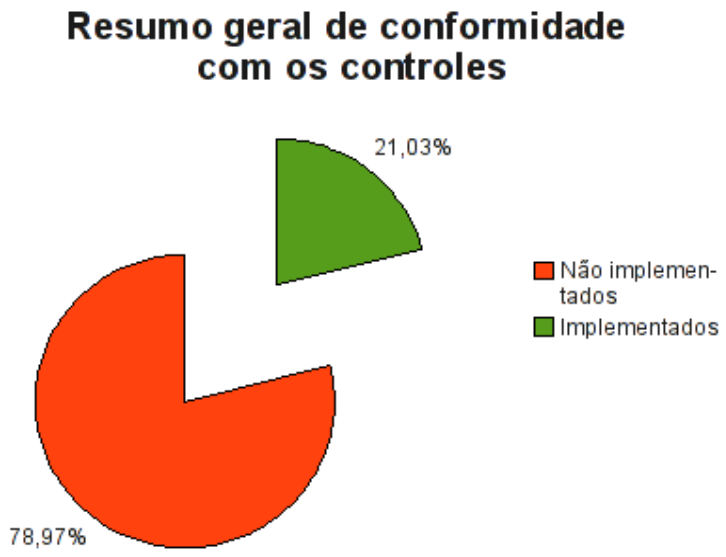


Figura 52: Resumo geral de conformidade com os controles de segurança

Na Tabela 76 (Custos e investimentos estimados necessários para mitigar/controlar os riscos) apresentamos o resumo dos custos e investimentos necessários para mitigar/controlar os riscos em cada um dos ativos analisados.

Tabela 76: Custos e investimentos estimados necessários para mitigar/controlar os riscos

Custos e investimentos estimados necessários para mitigar/controlar os riscos				
Ativo	***Risco (R$)***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Firewall Netfilter	1.155,00	1.050,00	2.410,00	4.615,00
Firewall Netfilter - controles do sistema operacional Linux	245,00	560,00	1.120,00	1.925,00
Servidor de banco de dados	700,00	8.560,00	44.560,00	53.820,00
Servidor de banco de dados - controles do sistema operacional *Windows* 2003 *Server*	210,00	280,00	4.130,00	4.620,00
Servidor ERP	5.040,00	26.760,00	23.680,00	55.480,00
Servidor ERP - controles do sistema operacional *Windows* 2003 *Server*	210,00	280,00	4.130,00	4.620,00
Servidor *Windows Active Directory*	0,00	0,00	7.030,00	7.030,00
Servidor *Windows Active Directory* - controles do sistema operacional *Windows* 2003 *Server*	210,00	280,00	4.130,00	4.620,00
Servidor de arquivos	0,00	1.540,00	1.330,00	2.870,00
Servidor de Arquivos - controles do sistema operacional *Windows* 2003 *Server*	210,00	280,00	4.130,00	4.620,00
Data center	0,00	7.360,00	7.800,00	15.160,00
Rede	30.620,00	93.000,00	13.200,00	136.820,00

Custos e investimentos estimados necessários para mitigar/controlar os riscos				
Ativo	***Risco (R$)***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Segurança física	13.920,00	25.560,00	0,00	39.480,00
Total (R$)	**52.520,00**	**165.510,00**	**117.650,00**	**335.680,00**

A implementação dos controles deverá seguir as determinações da metodologia.

8 ORÇAMENTO ANUAL DE TI

Na M2FE, o orçamento destinado à segurança da informação corresponde a um percentual do orçamento da área de tecnologia da informação.

Os investimentos relacionados à aquisição de novos equipamentos e *softwares* são debitados do orçamento do departamento solicitante, excetuando-se os investimentos realizados em infraestrutura e servidores, que são de responsabilidade do departamento de Tecnologia da Informação.

Na Tabela 77 (Orçamento de TI para os anos 2008 e 2009) são apresentados os custos e investimentos destinados à área de Tecnologia da Informação para os anos de 2008 e 2009. O aumento no orçamento de 2009 em relação à 2008 leva em consideração uma inflação de 8%. Observe que no orçamento de 2008 não há verba para a contratação do CSO, pois não havia previsão da necessidade de contratação do mesmo naquela época. O que ocorreu foi que, juntamente com a decisão da contratação do CSO, foi liberada uma verba em caráter emergencial para suprir esta necessidade durante o ano de 2008.

Tabela 77: Orçamento de TI para os anos 2008 e 2009

Custo							
Descrição		***2008***			***2009***		
		Mensal		***Anual***	***Mensal***		***Anual***
		qtde	***R$***	***R$***	***qtde***	***R$***	***R$***
Pessoal	Gerente	1	11.000	132.000	1	11.880	142.560
	Analista	1	7.000	84.000	1	7.560	90.720
	Administrador	1	7.000	84.000	1	7.560	90.720
	Help Desk	2	2.000	48.000	2	2.160	51.840
	CSO	0	0	0	1	13.000	156.000
	Sub-total			**348.000**			**531.840**
Infraes-estrutura	*Link* – 2Mbps *Internet*	1	2.300	27.600	1	2.300	27.600
	Link - *Speedy*	1	100	1.200			0
	Link - 256 Kbps	2	2.500	60.000	2	2.700	64.800
	Manutenção *Hardware*	1	1.000	12.000	1	1.080	12.960
	Manutenção *Software*	1	2.000	24.000	1	2.160	25.920
	Sub-total			**124.800**			**131.280**
Adminis-trativo	Escritório	1	500	6.000	1	540	6.480
	Consultoria Segurança	0	0	0	1	4.000	48.000
	Sub-total			**6.000**			**54.480**
Total de custo				**478.800**			**717.600**

Investimento anual					
Descrição		***2008***		***2009***	
		Anual		***Anual***	
		Qtde	***R$***	***Qtde***	***R$***
Investi-mento	Hardware	1	18.000	1	30.000
	Software	1	12.000	1	20.000
	Segurança	1	10.000	1	100.000
Total de investimento			**40.000**		**150.000**
Total Geral			**518.800**		**867.600**

9 REUNIÃO COM O PRESIDENTE

Terminada a análise de riscos, foi realizada uma reunião com o presidente da empresa para a apresentação do resumo executivo da análise de riscos, esclarecimentos a respeito de eventuais dúvidas sobre o processo de análise de riscos e sobre o panorama atual da empresa em relação à segurança da informação.

Durante a apresentação foi esclarecido ao presidente que os ativos, apesar de não estarem totalmente desprovidos de controles de segurança, apresentavam-se numa situação bastante preocupante, com mais de cinquenta por cento dos controles não implementados.

Durante esta reunião também foi salientado ao presidente a importância da implementação dos controles de segurança e que o orçamento previsto para a área de segurança da informação para o ano de 2009 era insuficiente, representando menos de trinta por cento do total necessário para a implementação de todos os controles. Sendo assim, foi solicitada uma verba adicional em caráter emergencial para permitir a implementação dos controles referentes aos riscos de intensidade alta, como uma forma de mitigar os riscos mais críticos e deixando os demais riscos para serem tratados futuramente, visto que o processo de segurança é cíclico, deve ser revisado anualmente e atualizado sempre que necessário.

Diante desta situação e dos prejuízos estimados com o incidente de segurança, o presidente decidiu manter o orçamento previsto para 2009 e fazer um aporte financeiro adicional para a segurança no valor de R$ 60.000,00 (sessenta mil reais), totalizando R$ 160.000,00 (cento e sessenta mil reais).

10 ESTRATÉGIA DE IMPLEMENTAÇÃO DOS CONTROLES

Como a nova verba destinada à segurança superava o valor necessário para a implementação de todos os controles dos riscos de alta intensidade, o excedente foi utilizado para implementar o *hardening* dos sistemas operacionais dos servidores e parte dos riscos de média intensidade, usando critérios técnicos, conforme apresentado na Tabela 78 (Controles implementados (exceto *hardening*)).

A seguir apresentamos os controles que foram implementados, conforme classificação por ativo, destacando o custo/investimento de cada controle bem como seu grau de risco.

Tabela 78: Controles implementados (exceto *hardening*)

Configurações	***Valor (R$)***	***Risco***	***Ativo***
Versão do *Netfilter* deve ser a versão estável mais atual.	70,00	Alto	*Firewall*
Apenas tráfego explicitamente autorizado deve ser permitido entre a DMZ e a *intranet.*	280,00	Alto	*Firewall*
Possui equipamento de reserva.	2.060,00	Alto	*Firewall*
Os registros de *log* do *Netfilter* devem ser analisados diariamente.	70,00	Médio	*Firewall*
Os arquivos de *log* devem ser rotacionados semanalmente.	280,00	Médio	*Firewall*
O encaminhamento IP (IP *Forward)* deve ser desabilitado enquanto as regras do *Netfilter* não tiverem sido carregadas.	35,00	Médio	*Firewall*

Configurações	***Valor (R$)***	***Risco***	***Ativo***
As regras devem impedir a saída de pacotes da rede interna com IPs públicos.	70,00	Médio	*Firewall*
O uso da diretiva *any* nas regras do *Netfilter* deve ser evitado ou minimizado.	35,00	Médio	*Firewall*
Versão do *software* deve ser a última disponível e compatível com o sistema.	14.800,00	Alto	DB
Aplicar as correções do banco de dados.	2.800,00	Alto	DB
A base de dados de desenvolvimento não deve conter dados de produção.	8.560,00	Alto	DB
Senhas criadas durante a instalação *(default)* devem ser substituídas.	280,00	Alto	DB
Senhas de conexão ao banco de dados devem estar de acordo com a política.	140,00	Alto	DB
O *Listener* deve exigir autenticação nas conexões.	560,00	Alto	DB
Desabilitar ou restringir os dispositivos de armazenamento (fita, CD, USB).	140,00	Alto	DB
A restauração do banco de dados deve ser restrita e autorizada aos administradores.	560,00	Alto	DB
Dados armazenados em *backup* devem ser cifrados.	12.800,00	Alto	DB
O acesso remoto (*Terminal Service*) deve ser restrito e controlados aos administradores.	280,00	Alto	DB
O tráfego de dados do banco de dados na rede deve ser cifrado.	2.800,00	Alto	DB
Não permitir acesso de analistas aos dados de produção.	560,00	Alto	DB
Os arquivos de trace só devem ser acessíveis pelo DBA.	280,00	Alto	DB

Configurações	*Valor (R$)*	*Risco*	*Ativo*
O servidor deve ser dedicado.	8.560,00	Médio	DB
O banco de dados do ERP não pode ser compartilhado com outras aplicações.	10.240,00	Alto	ERP
As senhas não devem ser armazenadas pelo sistema, apenas o *hash* das mesmas.	1.120,00	Alto	ERP
Todos os arquivos da aplicação ou criados pela mesma devem estar protegidos.	5.600,00	Alto	ERP
O controle de acesso da aplicação deve ser baseado em segregação de funções.	1.680,00	Alto	ERP
As contas de usuários devem ser desativadas após 3 tentativas consecutivas de acesso sem sucesso.	560,00	Alto	ERP
A comunicação entre a aplicação e o banco de dados deve ser cifrada.	2.800,00	Alto	ERP
O código da aplicação não deve ser mantido junto com a aplicação.	560,00	Alto	ERP
Verificar semestralmente se os *user IDs* são válidos, aprovados e com segregação de funções (auditoria).	1.120,00	Alto	ERP
Os arquivos de *log* devem ser rotacionados semanalmente.	280,00	Médio	ERP
Deve ser emitido aviso quando os *logs* estiverem a 80% da capacidade de saturação.	1.120,00	Médio	ERP
Habilitar política de histórico das últimas 5 senhas na política de domínio.	70,00	Alto	AD

Configurações	*Valor (R$)*	*Risco*	*Ativo*
Habilitar o requisito minimo de 15 caracteres para todas as contas administrativas.	70,00	Alto	AD
Restringir o acesso remoto aos servidores Controladores de Domínio aos administradores.	70,00	Alto	AD
Documentar todos servidores de AD e *Global catalog.*	560,00	Alto	AD
Documentar o FSMO (regras do domínio).	140,00	Alto	AD
Possuir pelo menos 2 servidores controladores de domínio trabalhando ativamente.	5.560,00	Alto	AD
As contas de serviço devem possuir nomes longos, com alta complexidade de senhas e não podem expirar.	140,00	Alto	AD
Garantir que os administradores possuem contas separadas para as atividades diárias e outra para as administrativas.	70,00	Alto	AD
Executar diariamente o *backup* da SAM e do *Schema Master.*	70,00	Alto	AD
Possuir ao menos 2 servidores habilitados com *Global Catalog* na floresta.	70,00	Alto	AD
Utilizar serviço NTP para sincronização de data e hora para todos os servidores.	140,00	Alto	AD
Garantir que todas as atualizações de segurança sejam instaladas.	70,00	Alto	AD
Documentar todas as unidades mapeadas, conforme sua função.	140,00	Alto	Servidor de arquivos

Configurações	*Valor (R$)*	*Risco*	*Ativo*
Deve ser fornecida área cifrada para armazenamento de arquivos classificados como confidenciais.	560,00	Alto	Servidor de arquivos
Garantir que o grupo *everyone* (todos) seja removido de todos os compartilhamentos.	140,00	Alto	Servidor de arquivos
Garantir que esteja sendo cumprida a política de *backup*.	70,00	Alto	Servidor de arquivos
Garantir que todos os arquivos de trabalho sejam gravados no servidor.	280,00	Alto	Servidor de arquivos
Limitar o tamanho do *Shadow Copies* para 20GB.	70,00	Alto	Servidor de arquivos
Auditar bimestralmente a conformidade de permissões com as definidas pela diretoria.	70,00	Alto	Servidor de arquivos
Todos os compartilhamentos devem ser documentados.	560,00	Médio	Servidor de arquivos
Todos os compartilhamentos devem ser ocultos.	140,00	Médio	Servidor de arquivos

Configurações	*Valor (R$)*	*Risco*	*Ativo*
A unidade pública deve ser apagada diariamente às 00h00.	70,00	Médio	Servidor de arquivos
Habilitar o recurso de *Shadow Copies* no volume onde os compartilhamentos estão criados.	140,00	Médio	Servidor de arquivos
Configurar o *Shadow Copies* para executar todos os dias da semana às 10h00 e às 15h00.	70,00	Médio	Servidor de arquivos
Deve ser definido e instalado um sistema de refrigeração de contingência para o *data center.*	7800,00	Alto	Data center
Remover do interior do *data center* todos os materiais não relacionados às atividades do mesmo.	560,00	Médio	Data center
A rede deve ser segmentada.	5.600,00	Alto	Rede
Devem ser Implementadas *Access Control List* entre *VLANs.*	2.800,00	Alto	Rede
Serviços acessíveis externamente devem estar na DMZ.	4.800,00	Alto	Rede
A função *anti-snooping* deve ser habilitada nos *switches*.	280,00	Médio	Rede
Todos os ativos de rede devem ter as senhas padrão alteradas.	560,00	Médio	Rede
Garantir que não existam *links* externos não gerenciados.	1.400,00	Médio	Rede
As áreas criticas devem possuir controle de acesso.	4560,00	Médio	Seg. Física
Devem haver câmeras de CFTV externas e internas e as imagens devem ser retidas por 30 dias.	20.800,00	Médio	Seg. Física

Configurações	*Valor (R$)*	*Risco*	*Ativo*
Os vidros da guarita de entrada devem ser escuros ou cobertos com película protetora escura.	200,00	Médio	Seg. Física

Considerando-se que os todos os servidores passaram pelo processo de *hardening* do sistema operacional, o resumo dos custos e investimentos aplicados na mitigação dos riscos é apresentado na Tabela 79 (Resumo dos custos e investimentos).

Tabela 79: Resumo dos custos e investimentos

Controles específicos dos ativos (exceto *hardening)*	139.800,00
Hardening de sistema operacional *Windows* - 4 servidores (R$4.620,00 cada)	18.480,00
Hardening de sistema operacional Linux – 1 servidor	1.925,00
Investimento Total (R$)	**160.205,00**

Para facilitar a visualização dos recursos financeiros empregados na mitigação dos riscos, a Tabela 80 (Investimento financeiro para mitigar/controlar os riscos) apresenta os valores de acordo com a intensidade dos riscos. Observe que os controles que combatem os riscos de baixa intensidade que aparecem na tabela referem-se aos processos de *hardening* dos sistemas operacionais.

Tabela 80: Investimento financeiro para mitigar/controlar os riscos

Investimento financeiro para mitigar/controlar os riscos				
Ativo	***Risco (R$)***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Firewall Netfilter	0	490	2.410	2.900
Firewall Netfilter - controles do sistema operacional Linux	245	560	1.120	1.925
Servidor de banco de dados	0	8.560	44.560	53.120
Servidor de banco de dados - controles do sistema operacional *Windows* 2003 *Server*	210	280	4.130	4.620
Servidor ERP	0	1.400	23.680	25.080
Servidor ERP - controles do sistema operacional *Windows* 2003 *Server*	210	280	4.130	4.620
Servidor *Windows Active Directory*	0	0	7.030	7.030
Servidor *Windows Active Directory* - controles do sistema operacional *Windows* 2003 *Server*	210	280	4.130	4.620
Servidor de arquivos - controles do sistema operacional *Windows* 2003 *Server*	210	280	4.130	4.620
Servidor de Arquivos	0	980	1.330	2.310
Data center	0	560	7.800	8.360
Rede	0	2.240	13.200	15.440
Segurança física	0	25.560	0	25.560
Total (R$)	**1.085**	**41.470**	**117.650**	**160.205**

Todos os servidores passaram pelo processo de *hardening* de sistema operacional, conforme os *checklists* apresentados na Tabela 81 (Controles do sistema operacional Linux) e Tabela 82 (Controles do sistema operacional W*indows* 2003).

Tabela 81: Controles do sistema operacional Linux

#	***Controle***
1	Instalar as correções de segurança sempre que disponibilizadas pelo fabricante.
2	Habilitar o uso do PAM *(Pluggable Authentication Modules)*.
3	Desabilitar o serviço *portmap* se o servidor não utilizar NFS.
4	Limitar o número de processos que um usuário pode executar simultaneamente.
5	Remover os serviços não necessários para a função do servidor (FTP, DNS, Apache etc).
6	Desabilitar o acesso da conta *root* nos consoles locais.
7	Criar contas com privilégios mínimos para os administradores e adicioná-las no grupo *wheel*.
8	Permitir a elevação de privilégios através do comando su somente ao grupo *wheel.*
9	Forçar o serviço SSH a aceitar conexões usando apenas a versão 2 do protocolo.
10	Adicionar apenas as contas dos administradores no grupo *wheel.*
11	Desabilitar o acesso da conta *root* via SSH.
12	Remover *banners* de identificação dos serviços habilitados.
13	Habilitar o registro de acessos de usuários (arquivos wtmp e btmp).
14	Habilitar log do sistema, separando por tipo de serviço.

15	Desabilitar os privilégios SUID e SGID dos programas não essenciais à função do servidor.
16	Habilitar o flag tcp_syncookies no TCP/IP para combater ataques do tipo *synflood*.
17	Desabilitar a resposta a requisições ICMP em *broadcast* (*ignore_broadcasts*=1).
18	Desabilitar o aceite de pacotes IP roteados pela origem (*.*accept_source_route*=0).
19	Habilitar a verificação de caminho reverso para combater ataques de IP spoofing (*rp_filter=1).
20	Adicionar as opções de montagem *nosuid* e *noexec* nas partições de dados (/home, /var etc).
21	Adicionar as opções de montagem *nosuid*, *noexec*, *nodev* à partição /tmp.
22	Adicionar as opções de montagem *nodev*, *noexec* e *nosuid* às mídias removíveis (*fstab*).
23	Ajustar o tempo de ociosidade do console para 5 minutos.
24	O *layout* de particionamento do disco deve ser adequado (/boot, /, /home, /usr, /var, /tmp etc).
25	Desabilitar desligamento do computador via CTRL+ALT+DEL.
26	Remover o ambiente gráfico se ele não for estritamente necessário ao funcionamento de alguma aplicação.
27	Habilitar o registro de eventos de uso do sistema (sysstat - comando sar).
28	Habilitar o *sticky bit* nos diretórios públicos (/tmp por exemplo).
29	Remover o suporte aos arquivos .rhosts do PAM.
30	Restringir o acesso ao agendador de tarefas (cron e at) apenas aos usuários autorizados.

31	Definir e habilitar senha no gerenciador de inicialização (GRUB/Lilo) para restringir o acesso ao modo monousuário.
32	Garantir que não haja nenhuma conta de usuário ativa com senha nula.
33	Os diretórios dos usuários (/home) devem possuir atributos 0750 ou mais restritivos.
34	Ajuste a máscara padrão de criação de arquivos e diretórios para 0770 (não acessíveis globalmente).
35	Desabilitar a geração de *core dumps* quando programas são abortados.
36	Habilitar a notificação automática de novas correções críticas disponíveis.

Tabela 82: Controles do sistema operacional *Windows* 2003

#	***Controle***
1	Verificar se todas partições estão formatadas com NTFS.
2	Permitir apenas a instalação de *devices* com *driver* assinado digitalmente.
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).
4	Garantir que os logs de eventos sejam configurados de forma que quando atingir 60 MB sobrescreva os eventos se necessário.
5	Remover todos os compartilhamentos padrões.
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.
7	Remover o acesso anônimo aos compartilhamentos.
8	Garantir que o *firewall* local do *host* está habilitado.
9	Permitir autenticação somente em NTLMv2.

10	Garantir que a auditoria esteja habilitada.
11	Garantir que seja desabilitado a enumeração anônima da base de dados SAM.
12	Desabilitar a conta *guest.*
13	Renomear a conta do administrador.
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.
15	O parâmetro da registro RunAs deve ser removido de todas as sub-chaves da chave HKLM\Software\Classes\AppID.
16	Desabilitar a conta de usuário SUPPORT_388945a0, utilizada para suporte da Miscrosoft.
17	As informações importantes devem armazenadas em disco de maneira cifrada.
18	Desabilitar o *autorun* de todos os *drives.*
19	Garantir que todos os *patches* de segurança disponibilizado pelo fabricante estejam instalados.
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.
21	Habilitar a notificação automática de novas correções críticas disponíveis.
22	As permissões NTFS para o diretório %SystemRoot% devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.
23	Garantir que o *backup* siga as especificações da política de *backup.*
24	Garantir que o *Windows* 2003 *Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer um evento tipo erro.
25	O recurso se geração do arquivo de DUMP da memória deve ser desabilitado.
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.
27	Habilitar o SYSKEY.

28	Garantir que as configurações de rede estejam documentadas.
29	Configurar a proteção contra ataques SYN.
30	Configurar o número máximo de retransmissão de pacotes SYN antes de abortar para 3 vezes.
31	Os *log* de eventos devem ser verificados diariamente.
32	Configurar o não armazenamento das credenciais de autenticação ou do .NET *passports*.
33	Configurar o não armazenamento dos *hashes* das senhas do LAN Manager no SAM.
34	O desempenho do *Windows* 2003 *Server* deve ser monitorado semanalmente.
35	Desabilitar o botão de *shutdown* do servidor.
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.
37	O sistema não deve permitir o suporte remoto não solicitado.
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.
39	Desabilitar a instalação automática de qualquer componentes do *Windows*.
40	Garantir que o Disco de reparo de Emergência do *Windows* esteja atualizado.

A Tabela 83 (Mapeamento dos ativos proposto para a matriz) apresenta o novo mapeamento dos ativos, conforme Figura 56.

Tabela 83: Mapeamento dos ativos proposto para a matriz

Nome	*Endereço IP/Máscara*	*Tipo*	*Descrição*	*Local*	*Hardware*	*Software*
REDE PÚBLICA						
Roteador_sp_1	192.168.1.1/29	Rede	Roteador *Internet*	*Data center*	Cisco 1841	c1841-advsecurityk9-mz.124-3f.bin
REDE VoIP						
PABX_sp_1	172.20.1.2/28	Rede	PABX HG Siemens VoIP	*Data center*	Siemens *hipath*	Versão 4
VLAN 1 - Servidores e Ativos						
Roteador_sp_2	172.16.1.1/24	Rede	Roteador *Default Gateway*	*Data center*	Cisco 1751	c1751-ipbase-mz.123-3a.bin
Firewall_sp_1	172.16.1.2/24	Rede	*Firewall* Linux *Netfilter*	*Data center*	HP Proliant DL 380 G3	GNU/Linux Debian 4.0 (Etch)
Switch_sp_1	172.16.1.3/24	Rede	*Switch* dos servidores	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE

Switch_sp_2	172.16.1.4/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_3	172.16.1.5/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_4	172.16.1.6/24	Rede	*Switch* das estações de trabalho	*Data center*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_5	172.16.1.7/24	Rede	*Switch* das estações de trabalho da fábrica	*Rack_1*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Switch_sp_6	172.16.1.8/24	Rede	*Switch* das estações de trabalho do almoxa-rifado	*Rack_2*	Cisco 2960	c2960-lanbase-mz.122-40.SE
Domain_Server	172.16.1.20/24	Servidores	*Active Directory*	*Data center*	HP Proliant DL 380 G4	Windows 2003 SP2

Mail_Server	172.16.1.21/24	Servidores	Servidor de *e-mail*	*Data center*	HP Proliant DL 380 G4	Windows 2003 SP2 + Exchange 2003 SP2
ERP_Server	172.16.1.22/24	Servidores	Servidor de aplicação	*Data center*	HP Proliant DL 380 G5	Windows 2003 SP1 + ERP
DB_Server	172.16.1.23/24	Servidores	Servidor de banco de dados	*Data center*	HP Proliant DL 380 G3	Windows 2003 SP2 + Oracle 9i
Domain2_Server	172.16.1.24/24	Servidores	*Active Directory*	*Data center*	HP Proliant DL 380 G4	Windows 2003 SP2
Proxy_Server	172.16.1.25/24	Servidores	*Proxy*	*Data center*	HP Proliant DL 380 G3	GNU/Linux Debian 4.0 (Etch) + Squid
Printer_sp_01	172.16.1.40/24	Impresso-ras	Impressora *laser*	Dire-toria	HP Color LasertJet 2840	-
Printer_sp_02	172.16.1.41/24	Impresso-ras	Impressora *laser*	Dire-toria	HP-P3005DN	-

Printer_sp_03	172.16.1.42/24	Impressoras	Impressora *laser*	Administrativo / Financeiro	HP-P3005DN	-
Printer_sp_04	172.16.1.43/24	Impressoras	Impressora *laser*	Comercial	HP-P3005DN	-
Printer_sp_05	172.16.1.44/24	Impressoras	Impressora *laser* colorida	Comercial	HP Color LasertJet 2840	-
Printer_sp_06	172.16.1.45/24	Impressoras	Impressora *laser*	Engenharia	HP-P3005DN	-
Printer_sp_07	172.16.1.46/24	Impressoras	*Ploter*	Engenharia	HP Plotter 800	-
Printer_sp_08	172.16.1.47/24	Impressoras	Impressora a jato de tinta	Montagem	HP Deskjet 630c	-
Printer_sp_09	172.16.1.48/24	Impressoras	Impressora a jato de tinta	Almoxarifado	HP Deskjet 630c	-
Printer_sp_10	172.16.1.49/24	Impressoras	Impressora matricial	Faturamento	Epson DFX 8000	-
Printer_sp_11	172.16.1.50/24	Impressoras	Impressora *laser*	TI	HP-P3005DN	-
Printer_sp_12	172.16.1.51/24	Impressoras	Impressora *laser*	Assist. Técnica	HP-P3005DN	-

VLAN 2 - ESTAÇÕES DE TRABALHO						
DHCP	172.16.2.10/24 - 172.16.2.253/24	Estações de trabalho	Faixa de Distribui-ção DHCP	-	-	-
VLAN 3 - WIFI						
AP_sp_1	172.16.3.1/24	Rede	Rede sem fio	*Rack_1*	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
AP_sp_2	172.16.3.2/24	Rede	Rede sem fio	*Rack_2*	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
AP_sp_3	172.16.3.3/24	Rede	Rede sem fio	*Rack_3*	Cisco AP1242AG	AIR-AP1242AG-A-K9 V 12.3(8)
DHCP	172.16.3.10/24 - 172.16.3.253/24	Estações de trabalho	Faixa de distribuiçã o DHCP	-	-	-
DMZ - SERVIDORES PUBLICADOS						
WEB_Server	192.168.5.20/28	Servidores	Servidor Web	*Data center*	HP Proliant DL 380 G3	Windows 2003 SP1

MailGatetway_ Server	192.168.5.30/28	Servidores	*Anti Spam*	*Data center*	HP Proliant DL 380 G3	GNU/Linux Debian 4.0 (Etch)

11 POLÍTICAS DE SEGURANÇA

Numa tradução livre de (BARMAN, 2001): *"A Política de Segurança é composta por um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e serviços importantes para a empresa recebam a proteção adequada, de forma a garantir a sua confidencialidade, integridade e disponibilidade."*.

Trazendo isso para o mundo mais prático, a Política de Segurança da empresa define o conjunto de normas e procedimentos que devem ser seguidos para manutenção da segurança das informações da empresa. Este conjunto de normas e procedimentos deve ser formalizado e de conhecimento de todos os integrantes da empresa, sejam eles funcionários, sócios, acionistas ou terceiros, enfim, todos que fizerem uso ou forem responsáveis por quaisquer informações da empresa.

O incidente de segurança ocorrido na M2FE gerou muitos questionamentos da alta administração. Foram cobradas providências imediatas para o tratamento dos riscos de novos vazamentos de informações da empresa.

Sabedora que a segurança é um processo contínuo e cíclico, a M2FE iniciou o processo de padronização, desenvolvimento e publicação de suas políticas de segurança, com foco no incidente ocorrido.

11.1 Estratégias de Implantação

Alguns cuidados devem ser tomados na implantação da política de segurança da informação, conforme apresentado a seguir.

Deve ser constituído um comitê de segurança, que deverá ser formado por representantes de departamentos (CSO, Gerentes Administrativo Financeiro, Produção e Assistência Técnica

e TI) responsáveis pela manutenção da política de segurança. Deve-se lembrar que a segurança da informação é um processo cíclico e, como tal, deve ser revisado e atualizado anualmente ou sempre que necessário.

A política de segurança deve definir as regras e os controles básicos para o acesso e uso da informação, devendo ser clara e de fácil entendimento do seu público-alvo. É muito importante definir a abrangência da política de segurança da informação, de forma que seu escopo e público-alvo sejam bem definidos.

Uma vez elaborada a política de segurança, ela deve ser divulgada a todos os membros da empresa, sejam eles sócios, acionistas, funcionários ou terceiros. Para que a Política de Segurança tenha a força necessária para surtir efeito, ela deve contar com o apoio explícito da alta direção da empresa.

A empresa deve prover os recursos financeiros e humanos necessários à implantação da política de segurança.

Cumpridos estes itens básicos, a implantação deve iniciar com a disponibilização da política a todos, tanto em meio físico (impressa) como digital, de forma que ela possa ser acessada a todo e qualquer instante e de qualquer lugar da empresa. É importante que os locais onde a política esteja disponível sejam amplamente divulgados. As versões impressas devem ser disponibilizadas em pontos estratégicos da empresa, nos acervos documentais dos departamentos e no *backup site*. A versão eletrônica deve ser disponibilizada num repositório central indexado, de forma a facilitar a sua pesquisa e as formas de se chegar a este repositório devem ser divulgadas em todo o *site* da *intranet*, de forma a permitir acesso rápido ao repositório de políticas.

Uma vez disponibilizadas as políticas, todos os colaboradores devem ser informados da sua existência usando-se mecanismos que atinjam o maior público possível, tais como mensagens eletrônicas (*e-mails*) e cartazes expostos em locais estratégicos da empresa, como, por exemplo, pontos de café, salas de reunião departamentais etc.

É desejável que o primeiro treinamento seja presencial e que os colaboradores sejam apresentados oficialmente à política de segurança e capacitados nas mesmas. Também será possível efetuar o controle de recebimento da política de segurança, bem como a realização de avaliação que auxilia na percepção do entendimento e envolvimento do funcionário. Todas

as avaliações devem ser enviadas para o departamento de recursos humanos e devem fazer parte do prontuário do funcionário. Treinamentos periódicos poderão ser realizados através de palestras e mini-cursos presenciais, ou através de um sistema de *e-learning*, de acordo com a disponibilidade de recursos humanos e computacionais.

11.1.1 O programa de conscientização da necessidade de segurança

O programa de conscientização de segurança da informação é um conjunto de palestras, treinamentos, materiais publicitários e certificação, que foi planejado para promover e manter a segurança da informação na M2FE.

Objetivo deste programa é preparar os colaboradores para a implementação das políticas criadas pela empresa, treinando-os e certificando-os.

11.1.2 A implantação das políticas

Após a criação do comitê de segurança e a aprovação das políticas, foi iniciado o Programa de Treinamento e Conscientização da Necessidade de Segurança da Informação com o envio de um *e-mail* a todos os colaboradores da empresa contendo uma carta do presidente.

A M2FE contratou uma empresa especializada para realizar o treinamento inicial e capacitar o pessoal de TI para realizar internamente os treinamentos futuros.

A M2FE realizou um café da manhã no qual foram distribuídos panfletos explicativos e *mouse pads* contendo dicas de segurança. O presidente apresentou os membros do comitê de segurança e falou da importância da política de segurança enfatizando que o sucesso da implementação da política depende da colaboração de todos.

Na página inicial da Intranet, que todos os funcionários têm acesso, foi divulgado um aviso sobre as datas e horários dos treinamentos e nos quadros de avisos foram fixados panfletos informativos.

Para novos colaboradores, o treinamento das políticas será parte do processo de integração.

Anualmente será realizado um processo de reciclagem a todos os colaboradores, abordando uma revisão de todos os documentos da política de segurança, conforme seu ciclo de vida.

Um dos panfletos contém um diagrama no qual é apresentado o ciclo de desenvolvimento das políticas, de forma a deixar claro o processo a todos os colaboradores e, de certa forma, estimulá-los a entender o processo. Este diagrama é apresentado na Figura 53.

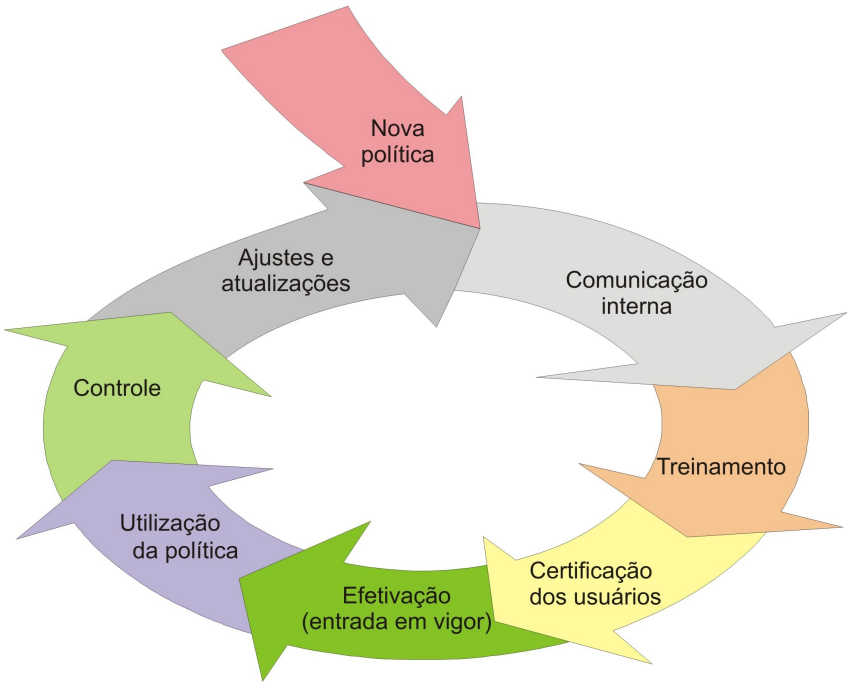


Figura 53: O ciclo de vida das políticas

O panfleto anunciando os treinamentos relacionados à segurança é apresentado na Figura 54.

Figura 54: Anúncio dos treinamentos de conscientização de segurança

Panfletos, como o mostrado na Figura 55 foram fixados em vários locais da empresa, como uma forma de conscientizar os colaboradores.

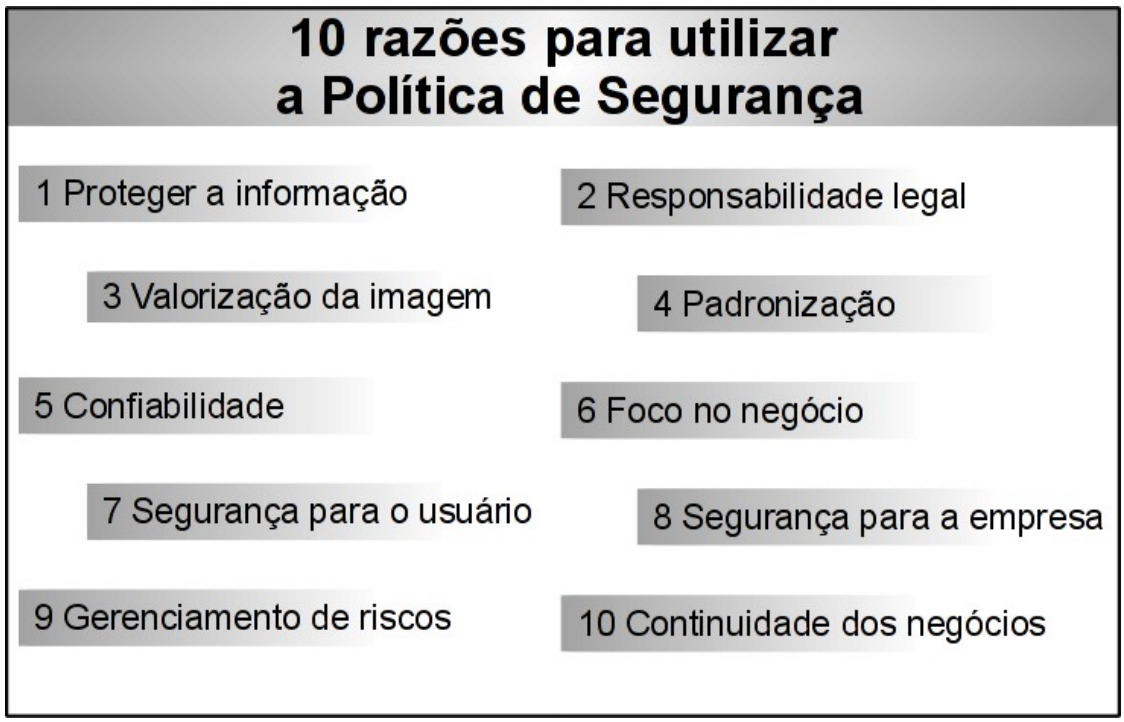


Figura 55: As dez razões da segurança

Como parte do plano de segurança, foram criadas:

- Carta de apoio do Presidente (Anexo A.1.1)
- Termo de responsabilidade, compromisso e sigilo (Anexo A.1.2)
- Diretrizes da Segurança da Informação (Anexo A.1.3)
- Políticas:
    - Política de uso da *Internet* (Anexo A.1.4.1)
    - Política de uso do correio eletrônico (Anexo A.1.4.2)
    - Política de uso de mídias removíveis (Anexo A.1.4.3)
    - Política de uso de dispositivos móveis (Anexo A.1.4.4)
    - Política de senhas (Anexo A.1.4.5)
    - Política de *backup* (Anexo A.1.4.6)
    - Política de uso de *software* (Anexo A.1.4.7)
    - Política técnica (Anexo A.1.4.8)
    - Política de classificação da informação (Anexo A.1.4.9)
- Procedimentos
    - Procedimento de reconfiguração de senha de usuário (Anexo A.2.1)
- Padrões de sistemas operacionais (Anexo A.3)

12 SEGURANÇA LÓGICA

Em linhas gerais, os controles que foram implementados oferecem as seguintes melhorias nos aspectos lógicos de segurança do ambiente:

- Instalação de *switch* core L3, criando 3 segmentos de rede (servidores e ativos, estações de trabalho e rede sem fio) e implementação de ACLs entre as VLANs, melhorando a segurança da rede.
- Remoção do *link* ADSL não gerenciado do escritório do Rio de Janeiro, eliminado vulnerabilidade de *link* não gerenciado.
- Criação de uma rede DMZ, para onde serão transferidos os servidores WEB e *gateway* de *e-mail*, pois ambos são acessados externamente.
- Instalação de um segundo controlador de domínio, melhorando a disponibilidade.
- Aquisição de um novo equipamento de reserva para o *firewall*.
- Atualização dos *softwares* essenciais dos ativos.
- Criação da documentação e procedimentos operacionais definindo as responsabilidades e tarefas.
- Criação de mecanismos de auditoria e rastreabilidade dos sistemas, através do uso de registros de *log*.
- Melhora na segurança dos sistemas básicos dos ativos através da execução de procedimentos de *hardening* dos sistemas operacionais.

- Segregação de acessos através da melhoria das definições de mecanismos de autenticação e perfis de usuário.

A estrutura lógica proposta para a rede é apresentada na Figura 56.

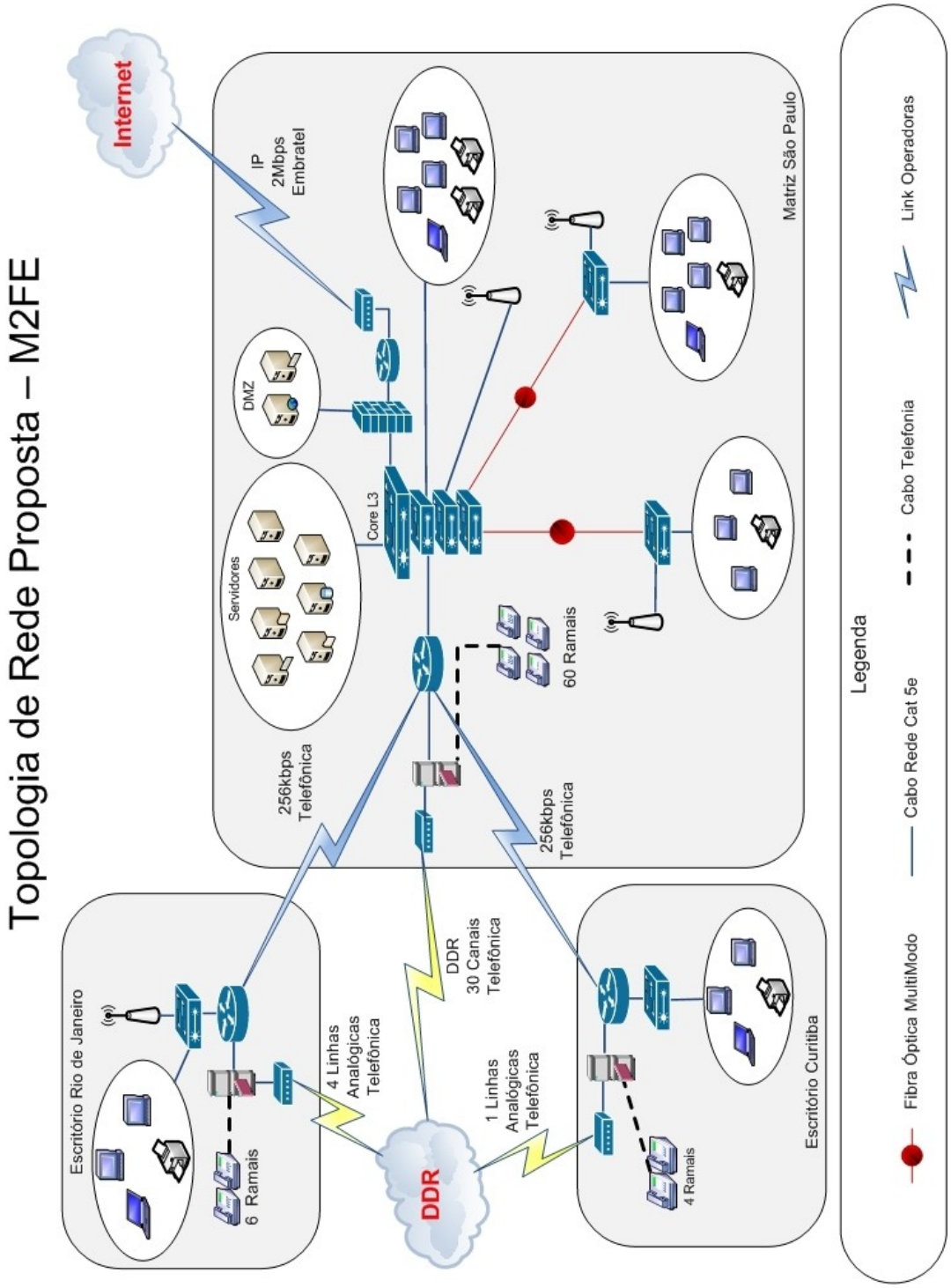


Figura 56: Estrutura lógica proposta para a rede

13 SEGURANÇA FÍSICA

A área da empresa foi dividida em três perímetros lógicos, a saber:

- Perímetro 3: é o mais externo, correspondendo aos limites físicos do terreno da empresa.
- Perímetro 2: compreende a parte do prédio da administração que provê acesso ao *data center*.
- Perímetro 1: sala do *data center*.

Estes perímetros foram criados com a finalidade de demarcar com maior clareza os caminhos para o acesso físico ao *data center*.

13.1 Perímetro 3

O perímetro 3 corresponde à área externa da empresa. Os limites físicos da empresa são demarcados com alambrados nas divisas laterais e nos fundos, com 3 fios de arame farpado na parte superior.

Nesta etapa do projeto de segurança, serão instaladas três câmeras de monitoração móveis (giratórias) em adição às já existentes, totalizando o total de seis câmeras de monitoração da parte externa da empresa. Estas novas câmeras serão integradas ao circuito de CFTV existente. As câmeras localizadas entre os dois prédios da empresa e a câmera localizada na parte frontal do prédio, com visada para portaria, serão mantidas.

Será instalada uma nova câmera na parte frontal da empresa, do lado oposto à portaria, com visada para a área frontal da empresa. Outras duas câmeras serão instaladas nos fundos da empresa, uma próxima à caixa d'água e outra no corredor do lado oposto.

Com estas seis câmeras será possível monitorar toda a área externa da empresa. A Figura 57 apresenta os limites lógicos do perímetro 3 e a disposição das câmeras.

A guarita da portaria terá todos os seus vidros cobertos com película protetora escura (*insulfilm)*.

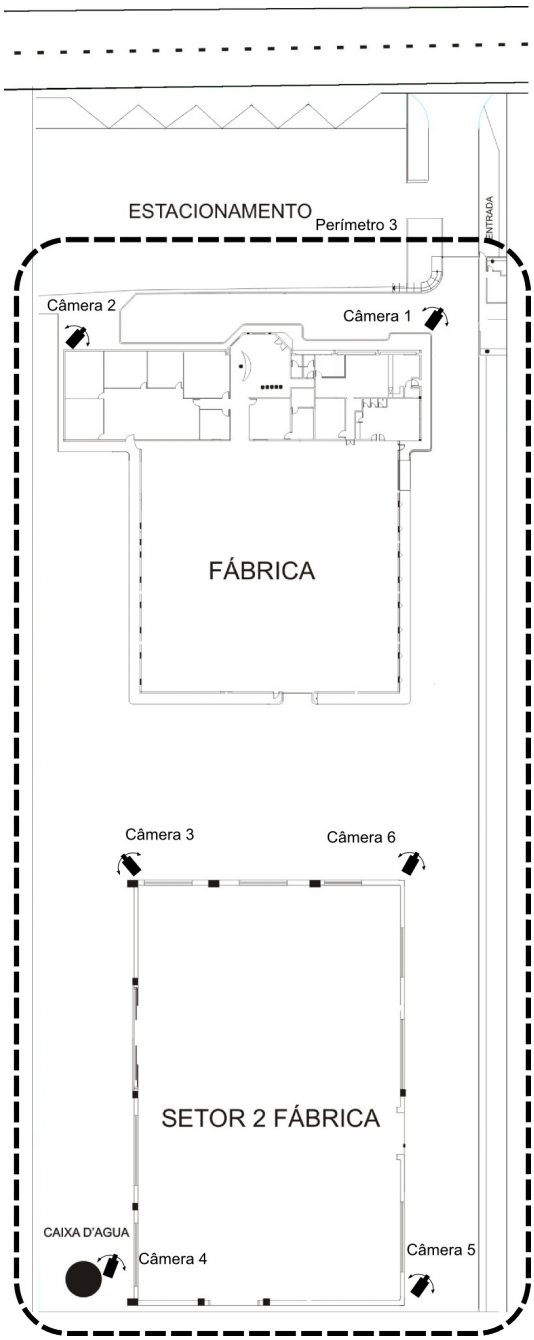


Figura 57: Perímetro 3

13.2 Perímetro 2

O perímetro de nível 2 compreende parte do prédio do escritório da empresa. Este perímetro foi assim demarcado por permitir uma visão geral do escritório ao redor do *data center*, com ênfase nos caminhos possíveis para acesso ao *data center*. A Figura 58 apresenta o perímetro 2.

Figura 58: Perímetro 2

Observe que a sala que antecede o *data center* é o único caminho de acesso ao mesmo e, nesta sala, serão instaladas uma catraca para controle de acesso e uma câmera para a monitoração com visada para a porta, onde se encontra a catraca. Estes controles visam restringir o acesso quanto mais próximo estivermos do *data center*.

13.3 Perímetro 1

O perímetro 1, ilustrado na Figura 59, compreende a sala do *data center*. Nesta sala serão instaladas uma câmera de monitoração com visada para a porta do *data center* e também uma fechadura eletrônica com acesso controlado por senha.

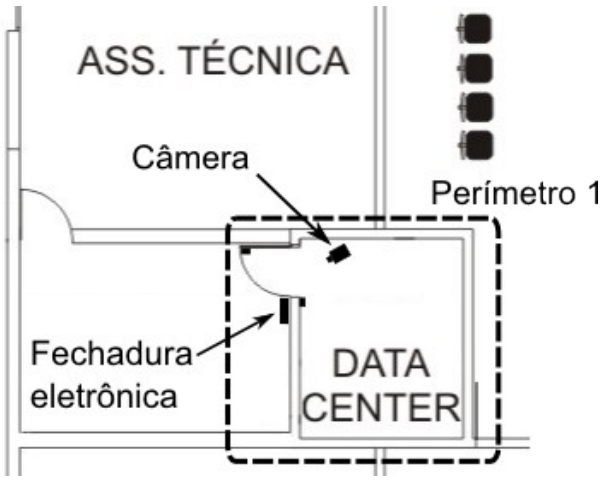


Figura 59: Perímetro 1

14 PLANO DE CONTINUIDADE DE NEGÓCIOS

O Plano de Continuidade de Negócios (PCN) é a disciplina que prepara preventivamente a organização de forma a manter vivos seus processos produtivos essenciais e recursos críticos interrompidos após a ocorrência de um desastre até o retorno à situação normal de funcionamento dentro do tempo aceitável.

A interrupção nos Processos de Negócios da empresa representa risco de perdas financeiras e de imagem e a insatisfação de seus clientes e investidores.

> *"No final do ano passado, foi publicado a primeira parte da norma britânica sobre Gestão de Continuidade de Negócios (GCN), a BS 25999, que especifica os requisitos de um plano para manter a operação em funcionamento em caso de alguma ocorrência. O seu objetivo é garantir que os sistemas fundamentais para a empresa retornem rapidamente à sua condição normal depois de ter passado por uma incidente de segurança, conseguindo, desta forma, minimizar os prejuízos".*
>
> *"Até dezembro de 2006, só existiam citações sobre contingenciamento em outras regulamentações, como a de Segurança da Informação prevista na NBR ISO/IEC 17799:2005, o modelo de boas práticas Cobit, entre outros. "Segundo os especialistas, a BS 25999 é a única norma mundial sobre continuidade dos negócios apresentada até agora ao mercado."*
>
> Fonte: http://www.setrix.com.br/noticia.php?cdnoticia=97, acessado em 15/Abril/2009.

O principal objetivo do PCN na M2FE é evitar que suas atividades sejam interrompidas em caso de falhas ou desastres significativos, minimizando seus impactos. Esse plano deverá ser testado e revisado, se necessário, pelo menos uma vez ao ano.

14.1 Lucros cessantes e *backup site*

Para fins de PCN a empresa M2FE foi dividida em duas áreas distintas: a área administrativa e financeira e a área de produção e montagem. A empresa possui seguro contra lucros cessantes, pois o custo anual para manter uma área de *backup site* é extremamente elevado se comparado ao custo contratado do seguro.

Caso ocorra um incidente que impossibilite o retorno das operações da matriz por um período superior a 30 dias, a direção da M2FE buscará no mercado um novo local para a instalação de sua linha de montagem. Ficou definido que somente a área administrativa, financeira e comercial contará com uma área de *backup site*, devido ao fato desta área ser considerada pela diretoria como sendo o coração e o cérebro da empresa.

A M2FE adotará o modelo de *Cold-Site* que prevê um site remoto com equipamentos capazes de suportar os seus principais sistemas de produção, porém sem a instalação de seus sistemas aplicativos e bancos de dados, os quais deverão ser instalados quando do acionamento do Plano de Recuperação de Desastres (PRD) a partir do último *backup* disponível. Nesse ambiente o processo de recuperação deve iniciar a partir da instalação dos *softwares* e da restauração dos *backups* de banco de dados, ERP, *Active Directory* e arquivos.

O *backup site* das filiais é a matriz e o *backup site* da matriz localiza-se na Av. Iguatemi, 1000 – 5º andar, salas 50, 51 e 52, Campinas – SP. Este local é administrado pela empresa BackupSiteOne, que pode ser contatada pelo telefone 0800-123456, disponível 24 horas por dia, sete dias por semana. Uma vez acionado o *backup site*, a empresa BackupSiteOne disponibiliza um serviço de transporte para os envolvidos desde a M2FE até o local.

O *backup site* disponibiliza 20 mesas, com computadores e ramais telefônicos e um *data center* com capacidade para hospedar até 10 servidores. A empresa administradora do *backup site* disponibiliza toda a infraestrutura necessária, como *Internet* e telefonia.

A infraestrutura de *Internet* do *backup* site é composta por um *firewall* e um *gateway* de *e-mail* com filtro *anti*-s*pams* e anti-vírus.

As configurações do *firewall* e do *gateway* deverão seguir a política de segurança vigente, caso possível será estabelecida uma VPN com o *firewall* da matriz e todos os

recursos disponíveis serão utilizados através da VPN diminuindo o tempo de restauração dos sistemas críticos da M2FE.

O prazo previsto para restaurar todos os sistemas críticos para a M2FE no *backup site* é de até 48 horas.

14.2 Missão / Objetivo / Atividades da M2FE

A M2FE possui reputação em assegurar e satisfazer as exigências de seus clientes com produtos inovadores e de alta qualidade, por meio de tecnologia avançada e assistência técnica especializada, sempre aumentando o retorno sobre o investimento.

Garante que suas operações estejam devidamente documentadas, registradas nos sistemas internos, processadas conforme padrões estabelecidos pela M2FE Órgãos Reguladores e reconciliadas com os devidos sistemas externos.

A M2FE procura aperfeiçoar-se para atender seus clientes com excelência, oferecendo melhor suporte a clientes, parceiros e colaboradores através de constante treinamento de sua equipe.

14.3 Metodologia

A metodologia do Plano de Continuidade de Negócios da M2FE abrange um conjunto de planos no qual se encontram formalizados e detalhados os procedimentos a serem seguidos na ocasião de ocorrência de eventos que possam afetar algum componente do seu Processo de Negócio e que possam acarretar perdas financeiras.

Esses planos se complementam cada qual com objetivos específicos, partindo de uma mesma base de análise e metodologia, a saber:

- PAC – Plano de Administração de Crise
- PCO - Plano de Continuidade Operacional
- PRD - Plano de Recuperação de Desastres

Plano de Administração de Crise (PAC) – Tem o propósito de definir detalhadamente o funcionamento das equipes envolvidas na contingência antes, durante e depois da ocorrência do incidente. Este plano também define os procedimentos a serem executados no período de retorno à normalidade.

Plano de Continuidade Operacional (PCO) – Tem o propósito de definir os procedimentos para contingência dos ativos da empresa que suportam os seus processos de negócio, objetivando reduzir o tempo de espera previsto para estabelecimento da atividade definido pelos gestores.

Plano de Recuperação de Desastres (PRD) – Tem o propósito de definir o plano de restauração e recuperação dos componentes afetados e/ou danificados que suportam os processos de negócio a fim de restabelecer o ambiente e as condições originais de operação.

Cada um destes planos é focado em uma determinada variável de risco e em uma situação de ameaça ao negócio da empresa:

- O PAC é focado nas atividades que envolvem as respostas aos eventos.
- O PCO é focado nas atividades que garantem a realização dos processos.
- O PRD é focado na substituição ou reposição de componentes que foram danificados.

14.3.1 Considerações especiais da M2FE

Para a elaboração do PCN, foram seguidas as seguintes orientações da diretoria:

- O PCN foi elaborado de uma forma abrangente, de acordo com a política da empresa, de forma a assegurar a manutenção de seus negócios e objetivos e minimizar os potenciais prejuízos.
- Os serviços de TI são apenas parte do plano total.
- O PCN não é um problema específico da área de TI, mas de toda a empresa.

- O PCN deve suportar desde pequenos incidentes, tais como indisponibilidades de *links*, até mesmo desastres de grandes proporções.

- O PCN permitirá dar confiança a M2FE, investidores, clientes, parceiros e colaboradores.

- O PCN foi elaborado para organizar e agilizar os processos decisórios.

- Os Comitês do PAC e PRD terão autonomia de decisão desde que aprovada pelo Comitê do PCN.

- As simulações de incidentes para a validação do PCN e os respectivos treinamentos deverão ocorrer anualmente.

14.3.2 Lista de contatos para acionamento e os processos de negócios

A lista de contatos para acionamento da equipe de recuperação de negócios da empresa deve possuir as seguintes informações (Anexo A.5.1):

- Nome do responsável.

- Tipo do evento relacionado ao processo.

- Qual seu envolvimento com o evento.

- Quanto tempo para o acionamento.

- Cargo do responsável.

- Nome da área do responsável.

- Telefones de contato: comercial, residencial e celular.

- *E-mail* profissional e pessoal.

- Seu substituto em caso de não localização.

14.3.3 Equipamentos de redes

A lista dos servidores necessários para o acionamento da equipe de recuperação de negócios da empresa são os seguintes:

Nome do ativo: Conti_01

- Tipo: HP Proliant DL 380 G4.
- Descrição: Servidor para hospedar o *Active Directory* e o servidor de arquivos.
- Local: *Data center backup site.*
- Fornecedor: BackupSiteOne.
- Criticidade: Alto.
- Características de Hardware: *Intel Xeon processor* 3.6GHz com 1MB *L2 Cache* 800MHz *Front Side Bus*, 4GB PC2-3200 DDR-2 SDRAM, 800 GB HD.
- Características de S.O.: *Windows Server* 2003 STD Inglês, SP2.
- Processo de Negócio suportado: Vendas, PCP e Compras.
- Tempo suportável em caso de falhas: 12 horas.
- Procedimento a ser utilizado no evento: Restauração do *backup.*

Nome do ativo: Conti_02

- Tipo: HP Proliant DL 380 G4.
- Descrição: Servidor de banco de dados.
- Local: *Data center backup site.*
- Fornecedor: BackupSiteOne.
- Criticidade: Alto.

- Características de Hardware: *Intel Xeon processor* 3.6GHz com 1MB L2 *Cache* 800MHz *Front Side Bus*, 4GB PC2-3200 DDR-2 SDRAM, 800 GB HD.
- Características de S.O.: *Windows Server* 2003 STD Inglês, SP2.
- Processo de Negócio suportado: Vendas, PCP e Compras.
- Tempo suportável em caso de falhas: 12 horas.
- Procedimento a ser utilizado no evento: Restauração do *backup.*

Nome do ativo: Conti_03

- Tipo: HP Proliant DL 380 G4.
- Descrição: Servidor de ERP.
- Local: *Data center backup site.*
- Fornecedor: BackupSiteOne.
- Criticidade: Alto.
- Características de Hardware: *Intel Xeon processor* 3.6GHz com 1MB L2 *Cache* 800MHz *Front Side Bus*, 4GB PC2-3200 DDR-2 SDRAM, 800 GB HD.
- Características de S.O.: *Windows Server* 2003 STD Inglês, SP2.
- Processo de Negócio suportado: Vendas, PCP e Compras.
- Tempo suportável em caso de falhas: 12 horas.
- Procedimento a ser utilizado no evento: Restauração do *backup.*

Nome do ativo: Conti_04

- Tipo: HP Proliant DL 380 G4.
- Descrição: Servidor de *e-mail.*
- Local: *Data center backup site.*

- Fornecedor: BackupSiteOne.
- Criticidade: Alto.
- Características de Hardware: *Intel Xeon processor* 3.6GHz com 1MB L2 *Cache* 800MHz *Front Side Bus*, 4GB PC2-3200 DDR-2 SDRAM, 800 GB HD.
- Características de S.O.: *Windows Server* 2003 STD Inglês, SP2.
- Processo de Negócio suportado: Vendas, PCP e Compras.
- Tempo suportável em caso de falhas: 12 horas.
- Procedimento a ser utilizado no evento: Restauração do *backup.*

14.3.4 Lista de Fornecedores

A lista deve contemplar os principais fornecedores que suportam a empresa e conter as seguintes informações (Anexo A.5.2):

- Razão Social.
- Endereço.
- Telefone.
- *E-mail.*
- Contato.
- Produto/Serviço.

Nota: nas futuras referências a fornecedores, os mesmos não serão nominados, sendo tratados genericamente, como por exemplo: fornecedor de *link,* fornecedor de servidor etc.

14.3.5 Lista de Materiais

A lista deve contemplar a relação de materiais essenciais para o início das operações da empresa e deve possuir as seguintes informações (Anexo A.5.3):

- Nome do Material.
- Especificação do material.
- Quantidade a ser solicitada.

14.3.6 Lista de Hardware e Software

A lista deve contemplar a relação de *Hardware* e *Softwares* essenciais para o início das operações da empresa e deve possuir as seguintes informações (Anexo A.5.4):

- Nome do *hardware* ou *software.*
- Quantidade.
- Principais fornecedores.

14.3.7 Documentos e procedimentos

Os documentos, relatórios e procedimentos deverão estar disponíveis em duas cópias, uma na matriz e outra no escritório de contingência.

- Documentos.
- Relatórios.
- Procedimentos.
- PCN.

14.3.8 Procedimentos para problemas em operações de emergência

Após identificar e compreender o problema, o plano entra em vigor a partir do momento que for declarado pelo Comitê do PCN, a ocorrência de um incidente, e somente após a declaração de normalidade do ambiente, o incidente e o plano poderão ser dados como encerrados.

Durante a execução do plano os participantes devem ser lembrados de como se comportar durante o incidente.

14.3.9 Retorno das operações

O processo de retorno das operações é realizado após os processos emergenciais e operacionais. É o processo de fechamento do ciclo do PCN, quando é verificada a normalidade das atividades da empresa após o evento. Esse processo deve ser concebido para acontecer imediatamente ou no menor tempo possível após a ocorrência do incidente.

Nessa etapa são descritos os procedimentos de encerramento do evento. É assegurado que os processos estão prontos para ser executados corretamente e em sua totalidade, ou seja, o ambiente está pronto para o seu perfeito funcionamento. Nessa etapa é feita a divulgação da situação de controle e de retorno à normalidade.

Após o retorno à normalidade, deverá ser analisado pelos responsáveis dos processos e pelos agentes de segurança, se os planos de ações referentes à recuperação foram efetivos ou se devem ser melhorados.

14.4 Acionamento do PCN

Antes mesmo de tratarmos o acionamento do PCN, devemos deixar claro que os documentos dos planos que o compõe devem estar em locais seguros, certos e sabidos para que todos os envolvidos possam tomar as medidas cabíveis. Os planos podem estar impressos ou até mesmo em meio magnético desde que devidamente acessíveis no momento da ocorrência, para todos os envolvidos no processo de recuperação.

Ao ser identificado que um incidente está em andamento, o Comitê do PCN deve ser acionado para que os responsáveis possam tomar as providências pré-estabelecidas no plano.

Nessa fase são iniciados os procedimentos de resposta emergencial, indicados no Plano de Administração de Crises e as equipes de emergência são acionadas. Após a avaliação dos

danos e tempo de previsão de parada, é decidido se o evento deve ser caracterizado como um desastre.

Se a resposta for afirmativa, é acionado o Plano de Recuperação de Desastres, caso contrário, a situação é estabilizada e volta a normalidade. Por exemplo:

- Se existir um problema com um determinado *hardware* de baixa criticidade provavelmente o próprio gerente de TI terá autonomia de ação bastando comunicar o Comitê de Gestão.

- Caso ocorra um incêndio, os níveis de ação estão restritos aos descritos no PCN.

Face ao exposto, a diretoria da M2FE definiu que se o desastre afetar apenas uma área, o gerente da área afetada (que também é membro do Comitê do PCN) fará a comunicação ao Comitê de Segurança e, se necessário, fará a comunicação ao Comitê do PCN que iniciará os procedimentos de contingência, dando assim uma maior autonomia e rapidez nas decisões.

Caso o desastre impacte um ou mais departamentos, o Gestor do PCN (CSO) e o Comitê de Segurança deverão ser acionados para as devidas providências.

Em todas as situações um relatório deverá ser enviado ao Comitê do PCN que o encaminhará ao Comitê de Segurança.

14.5 Definição dos papéis, responsabilidades e equipes

Com a finalidade de definir os envolvidos, definimos os papéis, responsabilidades e equipes envolvidos no PCN. Dado o pequeno porte da empresa, para o gerenciamento e acionamento dos planos, buscou-se manter comitês com um número mínimo, mas aceitável, de integrantes no qual, sempre que possível, os membros participam de mais de um comitê, viabilizando assim parte dos custos de manutenção dos planos.

14.5.1 Definição dos papéis e responsabilidades

Comitê de Decisão (Diretoria)

- Analisar estrategicamente e financeiramente o PCN.

- Aprovar o projeto do PCN.
- Aprovar o plano de atualizações do PCN.
- Patrocinar o PCN.

Comitê do Plano de Continuidade de Negócios

- Elaborar o projeto do PCN.
- Aprovar o projeto do PCN.
- Atualizar o projeto do PCN.
- Aprovar o projeto de atualizações do PCN.
- Patrocinar o PCN.

Gestor do PCN (CSO)

- Declarar os incidentes de alto impacto caso ocorram.
- Monitorar e gerenciar a execução dos planos do PCN e as equipes envolvidas.
- Garantir que os Planos do PCN sejam cumpridos de acordo com os prazos estabelecidos.
- Facilitar as ações e comunicações dos integrantes da equipe.
- Elaborar testes periódicos do PCN.
- Efetuar a comunicação pública no caso de desastre.
- Acionar pares e subordinados.

Comitê de Segurança (CSO)

- Elaborar o projeto do PCN.
- Elaborar o plano de atualizações do PCN.
- Divulgar o PCN.
- Aprovar comunicações.
- Garantir a atualização de informações do PCN.
- Atualizar políticas de segurança.
- Atualizar o Sistema de Gestão de Segurança da Informação.

Gerência Administrativa / Financeira

- Avaliar as potenciais perdas por atrasos oriundos de uma parada no sistema de informação.
- Elaborar a *Business Impact Analysis* (BIA).
- Facilitar as ações e comunicações dos integrantes de sua equipe.
- Elaborar e implementar as estratégias de divulgação, educação, conscientização e treinamento de todos os envolvidos no plano.
- Monitorar e gerenciar a sua equipe para a execução dos planos do PCN sob a sua responsabilidade.
- Acionar pares e subordinados.

Gerência de Produção e Assistência Técnica e Gerência de Engenharia

- Facilitar as ações e comunicações dos integrantes de sua equipe.

- Monitorar e gerenciar a sua equipe para a execução dos planos do PCN sob a sua responsabilidade.

- Adequar contratos com fornecedores de equipamentos e serviços para a adequação às necessidades do PCN.

- Acionar pares e subordinados.

Gerência de TI

- Garantir que as atividades de responsabilidade de sua área sejam cumpridas de acordo com os prazos estabelecidos.

- Adequar contratos com fornecedores de equipamentos e serviços para a adequação às necessidades do PCN.

- Monitorar e gerenciar a sua equipe para a execução dos planos do PCN sob a sua responsabilidade.

- Facilitar as ações e comunicações dos integrantes de sua equipe.

- Acionar pares e subordinados.

Gerência Comercial / Supervisores da área Industrial / Supervisores da área Administrativa / Financeira

- Facilitar as ações e comunicações dos integrantes de sua equipe.

- Monitorar e gerenciar a sua equipe para a execução dos planos do PCN sob a sua responsabilidade.

- Adequar contratos com fornecedores de equipamentos e serviços para a adequação as necessidades do PCN.

- Acionar pares e subordinados.

Brigada de Incêndio

- Garantir a integridade física das pessoas.
- Ativar o plano de evacuação do prédio.
- Ativar o plano de prevenção de incêndio caso necessário.

Agentes de Segurança (todos os gerentes e supervisores)

- Identificar o incidente ou receber a comunicação do incidente.
- Acionar a Brigada de Incêndio caso necessário.
- Garantir a segurança física dos ativos na Matriz.
- Garantir a segurança física dos ativos no *backup site*.
- Garantir o transporte de pessoas e equipamentos e documentos e outros elementos necessários ao funcionamento do *backup site.*

Grupo Funcional de Comunicação

- Elaborar o plano de comunicação.
- Elaborar comunicações.
- Garantir as comunicações do PCN.
- Garantir as comunicações dos eventos.

Grupo Funcional de Infraestrutura

- Elaborar necessidades de infraestrutura.
- Adquirir infraestrutura.
- Garantir as infraestruturas necessárias ao PCN.
- Implementar a infraestrutura.
- Garantir a infraestrutura durante o incidente.

Grupo Funcional de Operação

- Elaborar o plano de operação.
- Atualizar o plano de operação.
- Garantir as operações durante o incidente.

14.5.2 Grupo de Gestão

- Diretoria
    - Industrial.
    - Comercial.
    - Administrativa / Financeira.
- CSO.

14.5.3 Grupos Funcionais

Industrial

- Gerente de Produto e Assistência Técnica.
- Gerente de Engenharia.
- Supervisor de Produção.
- Supervisor de Assistência Técnica.

Comercial

- Gerente Comercial Matriz.
- Administrativo Financeiro.
- Gerente Administrativo Financeiro.
- Supervisor Administrativo.
- Supervisor Financeiro.
- Gerente de TI.

Direção

- CSO

14.5.4 Definição das equipes

14.5.4.1 Comitê de decisão

A Tabela 84 (*Comitê de decisão*) apresenta a relação de funcionários responsáveis pelo Comitê de decisão do PCN.

Tabela 84: Comitê de decisão

Nome	*Cargo*	*Telefone*
Funcionário1	Diretor Industrial	Telefone1
Funcionário2	Diretor Administrativo Financeiro	Telefone2
Funcionário3	Diretor Comercial	Telefone3

14.5.4.2 Comitê do PCN e Comitê de Segurança

A Tabela 85 (Comitê do PCN e Comitê de Segurança) apresenta a relação de funcionários responsáveis pelo Comitê do PCN e o Comitê de Segurança.

Tabela 85: Comitê do PCN e Comitê de Segurança

Nome	*Cargo/Função*	*Área*	*Telefones*	*Poder*
Funcionário4	Gestor do PCN (CSO)	Segurança da Informação	Telefone4	Decisão
Funcionário5	Gerente	Administrativo-Financeiro	Telefone5	Decisão
Funcionário6	Gerente	Produção e Assistência Técnica	Telefone6	Decisão
Funcionário7	Gerente	TI	Telefone7	Decisão

14.5.4.3 Grupo funcional: Operação

A Tabela 86 (Grupo funcional: Operação) apresenta a relação de funcionários responsáveis pelo grupo funcional Operação.

Tabela 86: Grupo funcional: Operação

Nome	*Cargo/Função*	*Área*	*Telefones*	*Poder*
Funcionário7	Gerente	TI	Telefone7	Execução
Funcionário8	Gerente	Engenharia	Telefone8	Execução
Funcionário9	Supervisor	Produção	Telefone9	Execução
Funcionário10	Supervisor	Assistência técnica	Telefone10	Execução
Funcionário11	Supervisor	Administrativa	Telefone11	Execução
Funcionário12	Supervisor	Financeira	Telefone12	Execução

14.5.4.4 Grupo funcional: Infraestrutura

A Tabela 87 (Grupo funcional: Infraestrutura) apresenta a relação de funcionários responsáveis pelo grupo funcional – Infraestrutura.

Tabela 87: Grupo funcional: Infraestrutura

Nome	*Cargo/Função*	*Área*	*Telefones*	*Poder*
Funcionário10	Gestor do PCN (CSO)	Segurança da Informação	Telefone10	Execução
Funcionário7	Gerente	TI	Telefone7	Execução
Funcionário8	Gerente	Engenharia	Telefone8	Execução
Funcionário6	Gerente	Produção e Assistência Técnica	Telefone6	Execução

14.5.4.5 Grupo funcional: Comunicação

A Tabela 88 (Grupo funcional: Comunicação) apresenta a relação de funcionários responsáveis pelo grupo funcional – Comunicação.

Tabela 88: Grupo funcional: Comunicação

Nome	*Cargo/Função*	*Área*	*Telefones*	*Poder*
Funcionário4	Gestor do PCN (CSO)	Segurança da Informação	Telefone10	Execução
Funcionário5	Gerente	Administrativa / Financeira	Telefone5	Execução
Funcionário13	Gerente	Comercial	Telefone13	Execução

14.6 PAC – Plano de Administração da Crise

O propósito do PAC é definir o funcionamento das equipes envolvidas com o acionamento da contingência antes, durante e depois da ocorrência do incidente. Além disso, tem que definir os procedimentos a serem executados também no período de retorno à normalidade.

O comportamento da empresa na comunicação do fato à imprensa é um exemplo típico de tratamento dado pelo PAC, pois a imagem corporativa é um ativo valioso da M2FE e saber como reagir a uma crise, principalmente no relacionamento com a mídia, é fundamental para preservar a imagem da empresa.

14.6.1 Cenário: incidente nível de alerta primário

- Incidente Tratado: Nível de Alerta Primário
    - Interdição no Prédio da M2FE e/ou
    - Indisponibilidade de acesso ao prédio.

A Tabela 89 (Cenário: incidente nível de alerta primário) apresenta informações relativas ao Cenário: Incidente Nível de Alerta Primário.

Tabela 89: Cenário: incidente nível de alerta primário

Incidente Nível de Alerta Primário	***Prédio interditado ou indisponível***
Área	Todos os prédios da Matriz
Autor	M2FE
Contato principal	Funcionário1
Contato substituto	Funcionário2
Objetivo	Executar procedimento para Contingência

14.6.2 Distribuição do Plano

Arquivo Eletrônico

- Rede Corporativa – Intranet
- CD, junto ao Posto de Comando (*backup site*)

Papel

- Arquivo de controles internos junto a área do CSO.
- Junto ao Posto de Comando (*backup site*)

14.6.3 Descrição Sucinta

Declarada a contingência na M2FE pelo Gestor do PCN:

- Deslocar o pessoal do Grupo de Operações para o Posto de Comando (*backup site*).

14.6.4 Acionamento / Comitê do PCN

A Tabela 90 (Acionamento / Comitê do PCN) apresenta informações relativas ao Acionamento do Comitê do PCN.

Tabela 90: Acionamento / Comitê do PCN

Responsável pela Ativação	Gestor do PCN - CSO
Ambiente de Contingência	Escritório Iguatemi
Prazo da Operação	(4) horas
Posto do Comando	M2FE – Av. Iguatemi, 1000 5º. Andar, salas 50, 51 e 52 Fone 0800-123456

14.6.5 Fluxo de ações

A Tabela 91 (Prioridade de ação) apresenta as atividades a serem executadas pelo Comitê do PCN para o nível de alerta primário – Indisponibilidade de acesso.

Tabela 91: Prioridade de ação

Atividades a serem executadas pelo comitê do PCN para o nível de alerta primário – Indisponibilidade de acesso
A - Avaliação inicial da situação.
1. Após constatação do nível de alerta primário, os membros do comitê do PCN contatarão os colaboradores, informando aos mesmos a ação a ser tomada: • o retorno ao prédio ou • deslocamento para o site de contingência

Atividades a serem executadas pelo comitê do PCN para o nível de alerta primário – Indisponibilidade de acesso
2. Entrar em contato com o gestor do PCN (CSO) para verificar a previsão do tempo de indisponibilidade.
3. Caso o tempo de duração da paralisação seja superior ao admitido para o processo crítico, informar ao Comitê do PCN**.**
4. Comitê do PCN dá início às atividades do PCN – Plano de Continuidade de Negócios .
5. Ativar o site de contingência (Posto de comando).
6. Acionar os colaboradores dos grupos funcionais para o deslocamento para o Posto de Comando.
7. Informar a decisão aos demais colaboradores e informar sobre os procedimentos a serem adotados (aguardar ou dispensar).
8. Orientar o deslocamento dos colaboradores para o Posto de Comando.
9. Contatar os principais clientes (internos e externos) e informar os telefones que serão disponibilizados para contato.
10. Contatar os principais fornecedores interagindo com eles caso seja necessário.
11. Iniciar os trabalhos no *site* de contingência.
12. Monitorar a Situação. ● Membro do Comitê de Decisão mantém contato contínuo com o Gestor do PCN (CSO) para verificar a perspectiva e a estimativa de prazo para a normalização da situação ou liberação do prédio da matriz. ● O Gerente do Evento, após a liberação do prédio, decide se voltará às atividades normais e comunica ao líder da contingência.

Atividades a serem executadas pelo comitê do PCN para o nível de alerta primário – Indisponibilidade de acesso
13. Após a normalização da Situação: ● Contatar os colaboradores para o retorno ao prédio da matriz da M2FE. ● Realizar os procedimentos básicos para retomada das atividades no prédio da matriz. ● Informar, mediante reunião/relatório, o ocorrido e as soluções adotadas na contingência apresentando sugestões para aprimoramento do plano, enviando para o gestor do plano de continuidade de negócios.

14.6.6 Ambiente de contingência: contra-medidas/premissas

A Tabela 92 (Ambiente de contingência: contra-medidas/premissas) apresenta as alternativas possíveis em caso de um incidente.

Tabela 92: Ambiente de contingência: contra-medidas/premissas

Contra-Medidas (Medidas de Segurança)	*Premissas*
1 – Alternativa 1	Caso o evento ocorra em alguma filial: os funcionários principais deverão trabalhar na matriz. Contratação de Transporte e hospedagem para os funcionários.

Contra-Medidas (Medidas de Segurança)	*Premissas*
2 – Alternativa 2	Caso o evento ocorra na matriz e não afete toda a empresa: efetuar somente os recebimentos e pagamentos da M2FE enquanto o ambiente da matriz e/ou do Posto de Comando não estiver totalmente restabelecido.

14.6.7 Infraestrutura necessária

A Tabela 93 (Infraestrutura necessária) apresenta a infraestrutura mínima para atendimento do PAC.

Tabela 93: Infraestrutura necessária

Serviços Necessários	Contratação de Transporte
	Suporte para Alimentação
	Contratação de Hospedagem
Recursos Necessários	Material de Escritório
	Material para pagamentos e recebimentos (via Internet / cheque)
	5 Celulares
Hardware / Software	20 estações
	3 Impressoras
	5 telefones
	Sistema ERP (guardar *backup* em local externo à matriz – Banco de dados e arquivos)

	MS-Office
	2 *Notebooks*
Posto de Comando da M2FE	Av. Iguatemi, 1000 – 5º. Andar, salas 50, 51 e 52 *Help Desk:* Tel: 0800-123456 *E-mail*: helpdesk@m2fe.com.br

14.7 PCO – Plano de Continuidade Operacional

O Plano de Continuidade Operacional (PCO) tem o propósito de definir os procedimentos para contingenciamento dos ativos que suportam cada processo crítico de negócio, objetivando reduzir o tempo de indisponibilidade e, consequentemente, os impactos potenciais ao negócio devido à ocorrência de eventos previamente identificados e definidos.

Por intermédio do Plano de Continuidade Operacional, os gestores dos processos de negócios saberão como agir na falta ou falha de algum componente que suporte o processo, garantindo a continuidade do negócio e reduzindo o impacto na M2FE

O Plano de Continuidade Operacional deve ficar em local visível e acessível a todos, sendo a área de Tecnologia da Informação responsável pela sua atualização e execução.

A seguir serão apresentados:

- os principais ativos para contingenciamento
- os relacionamentos entre processos, sistemas e ativos
- a estrutura lógica da rede
- os procedimentos de contingenciamento dos ativos

14.7.1 Principais ativos para contingenciamento

O plano atende os tipos de paralisação previamente identificados e definidos na infraestrutura de TI. Os principais ativos de TI para situação de contingência são apresentados na Tabela 94 (Principais ativos de TI para situação de contingência).

A Tabela 94 (Principais ativos de TI para situação de contingência) apresenta a relação dos principais ativos de TI, seus responsáveis e a solução de contingência a ser adotada.

Tabela 94: Principais ativos de TI para situação de contingência

Ativo de TI	***Responsável***	***Solução de Contingência***
Link de dados	Funcionário11	SLA - *Cold Site*
Link de voz	Funcionário11	SLA - *Cold Site*
Infraestrutura de acesso à *Internet*	Funcionário11	SLA - *Cold Site*
Infraestrutura de rede	Funcionário11	SLA - *Cold Site*
Sistema ERP	Funcionário7	*Cold Site / Restore*
Sistema de arquivos	Funcionário7	*Cold Site / Restore*
Sistema de correio eletrônico	Funcionário6	*Cold Site / Restore*
Sistema de navegação na *Internet*	Funcionário6	*Cold Site / Restore*
Servidor ERP	Funcionário7	*Cold Site / Restore*
Servidor de Banco de Dados	Funcionário7	*Cold Site / Restore*
Servidor de arquivos	Funcionário6	*Cold Site / Restore*

Ativo de TI	*Responsável*	*Solução de Contingência*
Servidor de *e-mail*	Funcionário6	*Cold Site / Restore*
Firewall	Funcionário6	Redundância de *Firewall*
Servidor *Internet* (*web*)	Funcionário6	*Cold Site / Restore*
Servidor *Active Directory,* DHCP e DNS	Funcionário7	*Cold Site / Restore*
Roteador de *Internet*	Funcionário6	Redundância de roteador
Proxy	Funcionário6	Redundância de *proxy*

14.7.2 Relacionamentos entre processos, sistemas e ativos

A Figura 60 e a Figura 61 mostram graficamente todos os esquemas da rede local e das filiais, a infraestrutura de voz e de dados, os sistemas, processos e serviços de TI da M2FE, conforme identificados no processo de análise de riscos.

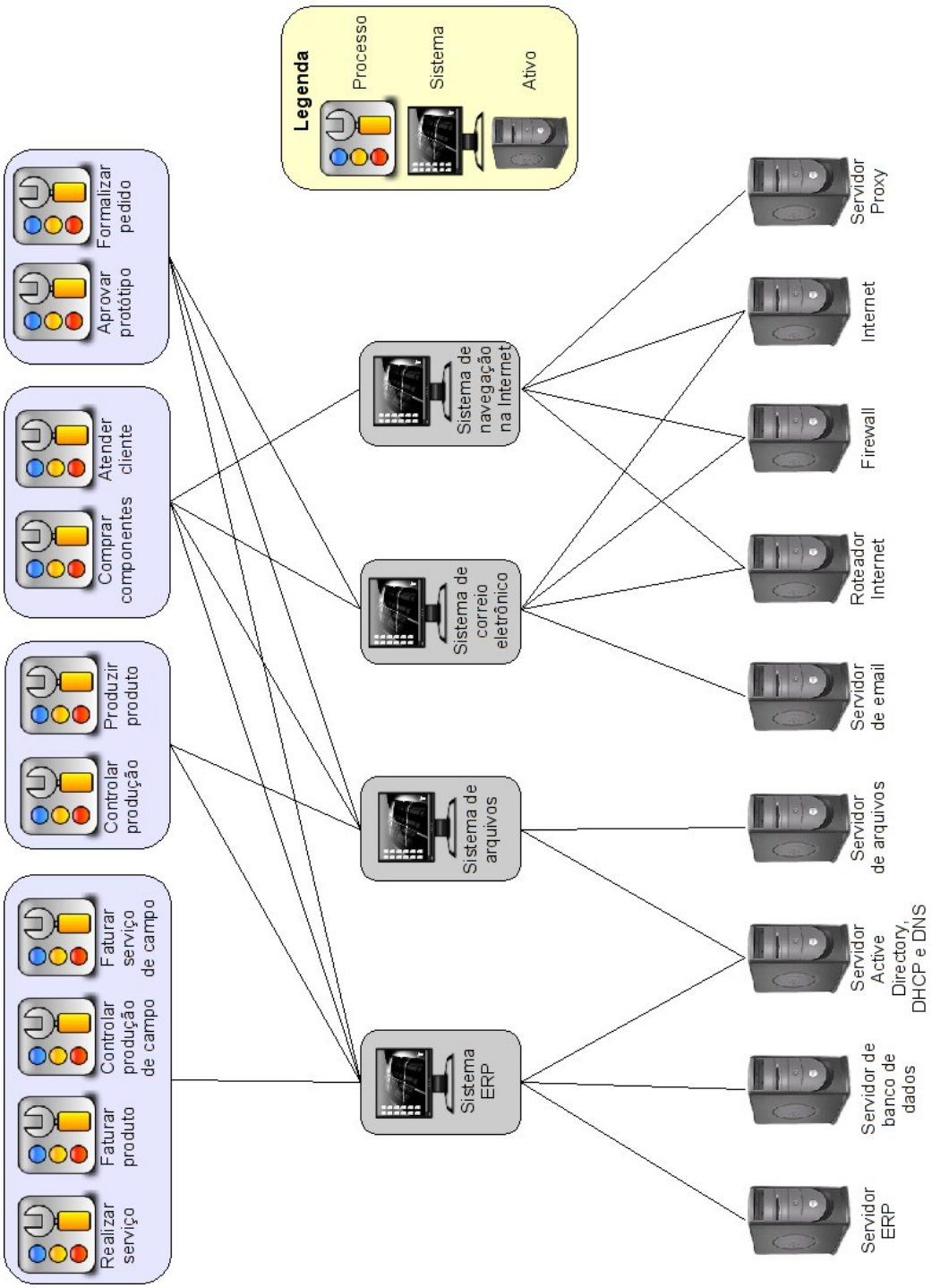


Figura 60: Macro Fluxo – TI: Sistemas, processos e ativos envolvidos

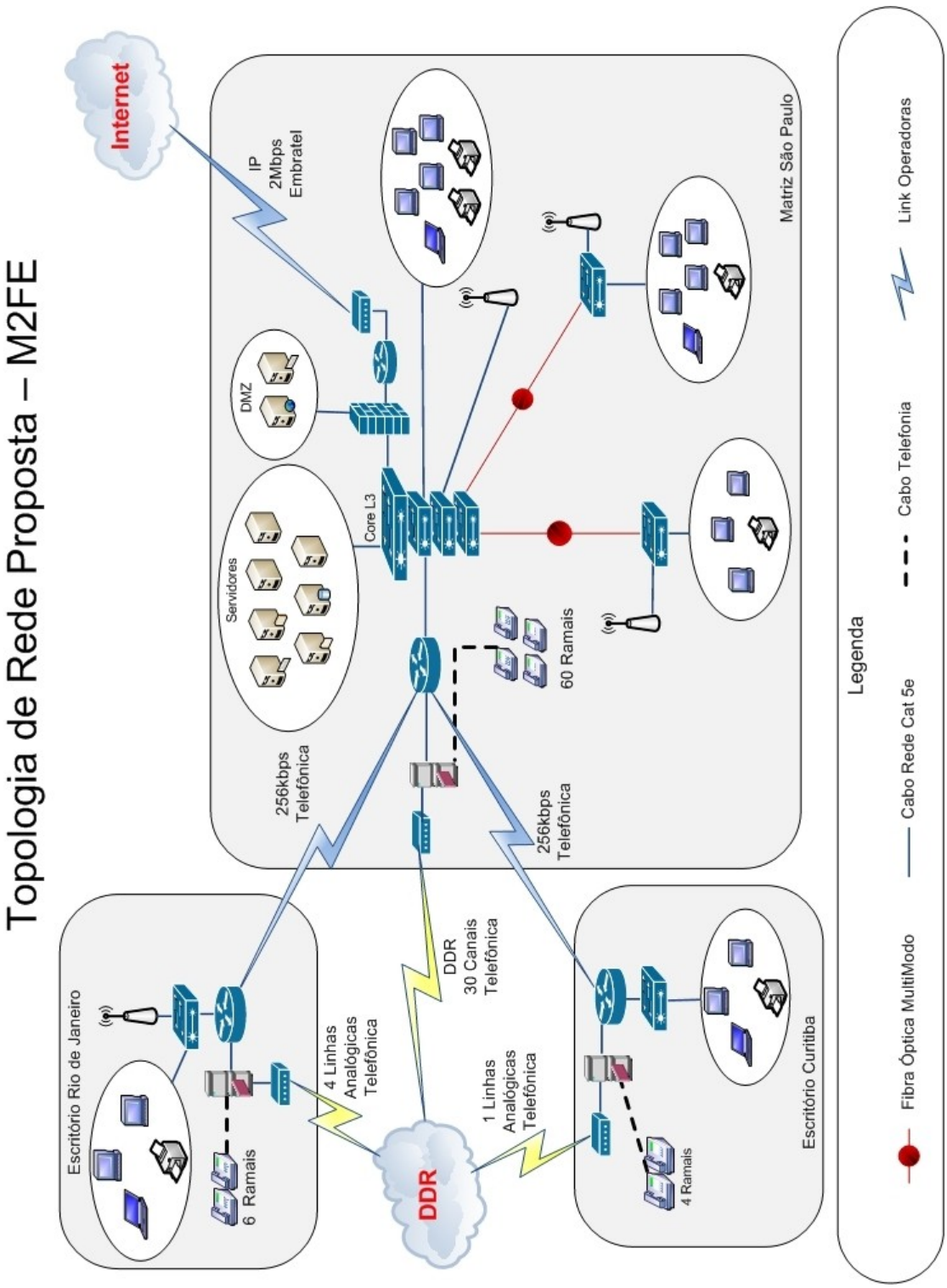


Figura 61: Estrutura lógica da rede

14.7.3 Infraestrutura de acesso à *Internet*

O que é

Infraestrutura de acesso e disponibilização de serviços de *Internet*, o acesso dispõe de *link* secundário.

O que compõe

- Infraestrutura elétrica.
- Infraestrutura de rede.
- *Link* de dados.
- *Firewall.*
- Roteador *Internet.*
- Servidor *Proxy.*
- *Switches.*

Fornecedores

- Fornecedores de *link*, roteadores e *switches*.
- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedor de *software.*

14.7.3.1 Riscos e impactos

A Tabela 95 (Riscos e impactos para a infraestrutura de acesso à *Internet*) apresenta a relação de riscos e seus devidos impactos.

Tabela 95: Riscos e impactos para a infraestrutura de acesso à *Internet*

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *Firewall*	Indisponibilidade de acesso a *Internet.* Mensagem de erro.
Falha no *link* de dados	Indisponibilidade de acesso aos sistemas. Mensagem de erro dos sistemas. Erro de acesso a rede.
Falha no *Proxy*	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha no roteador	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

14.7.3.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail* ou telefone .

14.7.3.3 Plano de testes

Testes de conectividade com a *Internet*.

14.7.4 Infraestrutura de rede

O que é

Infraestrutura de rede da M2FE, composta pelo cabeamento e pelos equipamentos de acesso básico, como roteadores, *switches* e servidores básicos.

O que compõe

- Infraestrutura elétrica.
- Infraestrutura de rede.
- *Link* de dados.
- *Switches.*
- Roteadores.
- *Firewall.*
- *Proxy.*

Fornecedores

- Fornecedores de *link*, roteadores e *switches.*
- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.

14.7.4.1 Riscos e impactos

A Tabela 96 (Riscos e impactos para a infraestrutura de rede) apresenta a relação de riscos e seus devidos impactos.

Tabela 96: Riscos e impactos para a infraestrutura de rede

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *Firewall*	Indisponibilidade de acesso a *Internet.* Mensagem de erro.
Falha no *link* de dados	Indisponibilidade de acesso aos sistemas. Mensagem de erro dos sistemas. Erro de acesso a rede.
Falha no *Proxy*	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha no roteador	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

14.7.4.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet*.

14.7.4.3 Plano de testes

Teste de conectividade com a rede da M2FE.

14.7.5 Sistema ERP

O que é

O sistema de ERP (*Enterprise Resource Planning*) ou SIGE (Sistemas Integrados de Gestão Empresarial) é o principal sistema da M2FE e integra as informações de diversas áreas como: Comercial, Engenharia de Produto e Aplicação, Compras, Financeira, Contábil entre outras. O sistema é executado através do arquivo ERP08.EXE que é compartilhado no servidor ERP.

Os aplicativos executados pela rede com acesso a banco de dados são os responsáveis pela gestão de negócios e gerenciamento da M2FE.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura da rede.
- Servidor de ERP.
- Servidor de banco de dados.
- Servidor de arquivos.
- Servidor *Active Diretory*, DHCP e DNS.
- Banco de dados (*software)*.

Fornecedores

- Fornecedor do sistema ERP.
- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedores de *software.*
- Fornecedor de banco de dados.

14.7.5.1 Riscos e impactos

A Tabela 97 (Riscos e impactos para o sistema ERP) apresenta a relação de riscos e seus devidos impactos.

Tabela 97: Riscos e impactos para o sistema ERP

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no banco de dados	Indisponibilidade de acesso ao banco de dados. Erro de acesso ao banco de dados. Erro de acesso ao servidor.

Riscos	*Impactos*
Falha no servidor AD, DHCP e DNS	Erro de *login.* Erro de acesso a rede. Erro de acesso aos servidores. Erro de acesso à *Internet.*
Falha no servidor de arquivos	Erro de acesso ao servidor. Erro de acesso aos arquivos. Indisponibilidade dos arquivos. Falha na restauração de arquivos.
Falha no servidor de banco de dados	Erro de acesso ao servidor. Erro de acesso ao banco de dados. Erro de acesso aos dados. Mensagens de erro. Indisponibilidade do servidor.
Falha no sistema ERP	Indisponibilidade de acesso ao sistema. Erro de acesso ao sistema. Erro de acesso ao servidor.

14.7.5.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet.*

14.7.5.3 Plano de testes

Testes de execução da aplicação e execução de operações do sistema.

14.7.6 Sistema de arquivos

O que é

O sistema de Arquivos da M2FE foi desenvolvido com a finalidade de gerenciar o armazenamento e a recuperação de documentos de forma eficiente, permitindo usar os arquivos diretamente no servidor como se estivessem em seu próprio microcomputador.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Sistema de arquivos.
- Servidor de Arquivos.
- Servidor *Active Diretory*, DHCP e DNS.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedores de *softwares.*

14.7.6.1 Riscos e impactos

A Tabela 98 (Riscos e impactos para o sistema de arquivos) apresenta a relação de riscos e seus devidos impactos.

Tabela 98: Riscos e impactos para o sistema de arquivos

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no servidor AD, DHCP e DNS	Erro de *login.* Erro de acesso a rede. Erro de acesso aos servidores. Erro de acesso à *Internet.*
Falha no servidor de arquivos	Erro de acesso ao servidor. Erro de acesso aos arquivos. Indisponibilidade dos arquivos. Falha na restauração de arquivos.
Falha no sistema de arquivos	Indisponibilidade de acesso ao sistema. Erro de acesso aos arquivos. Erro de acesso ao servidor.

14.7.6.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, via *e-mail*, telefone ou *Internet.*

14.7.6.3 Plano de testes

Teste de acesso ao sistema de arquivos (gravação e leitura de arquivos).

14.7.7 Sistema de correio eletrônico

O que é

O sistema de correio eletrônico da M2FE além de possibilitar o gerenciamento de envio e recebimento de *e-mails*, também possui algumas características específicas como catálogo de endereços e agenda corporativa.

É o principal meio de comunicação eletrônica entre colaboradores, fornecedores e clientes.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Infraestrutura de *Internet.*
- Servidor de *e-mail.*
- Roteador *Internet.*
- *Firewall.*
- Sistema de correio eletrônico.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*
- Fornecedor de servidores.
- Fornecedores de *software.*

14.7.7.1 Riscos e impactos

A Tabela 99 (Riscos e impactos para o sistema de correio eletrônico) apresenta a relação de riscos e seus devidos impactos.

Tabela 99: Riscos e impactos para o sistema de correio eletrônico

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso a *Internet.*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *Firewall*	Indisponibilidade de acesso a *Internet.* Mensagem de erro.
Falha no roteador	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

Riscos	*Impactos*
Falha no servidor de *e-mail*	Erro no sistema de *e-mail*. Indisponibilidade de acesso aos *e-mails*.
Falha no sistema de correio eletrônico	Indisponibilidade de acesso ao sistema. Erro de acesso ao *e-mail*. Erro de acesso ao servidor. Erro na atualização de *e-mails*.

14.7.7.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por telefone ou *Internet.*

14.7.7.3 Plano de testes

Testar o funcionamento através do envio e recebimento de mensagens internamente e através da *Internet*.

14.7.8 Sistema de navegação na Internet

O que é

O sistema de navegação na *Internet* é formado pelos *softwares* e recursos básicos usados para acesso à *Internet*.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica

- Infraestrutura de rede.
- Infraestrutura de *Internet.*
- Roteador *Internet.*
- *Firewall.*
- Servidor *Internet.*
- *Proxy.*

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*
- Fornecedor de servidores.
- Fornecedores de *software.*

14.7.8.1 Riscos e impactos

A Tabela 100 (Riscos e impactos para o sistema de navegação na *Internet*) apresenta a relação de riscos e seus devidos impactos.

Tabela 100: Riscos e impactos para o sistema de navegação na Internet

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso a *Internet.*

Riscos	*Impactos*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *Firewall*	Indisponibilidade de acesso a *Internet.* Mensagem de erro.
Falha no *proxy*	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha no roteador	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha no servidor de *Internet*	Erro de acesso ao servidor. Erro de acesso às páginas. Indisponibilidade do servidor.

14.7.8.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet*.

14.7.8.3 Plano de testes

Testar a conectividade através do acesso de *sites* disponíveis na *Internet*.

14.7.9 Servidor ERP

O que é

É o servidor onde estão instalados os executáveis do sistema ERP.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Servidor de banco de dados.
- Servidor ERP.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedores de *software.*
- Fornecedor de banco de dados.
- Fornecedor do sistema ERP.

14.7.9.1 Riscos e impactos

A Tabela 101 (Riscos e impactos para o servidor ERP) apresenta a relação de riscos e seus devidos impactos.

Tabela 101: Riscos e impactos para o servidor ERP

Riscos	*Impactos*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no banco de dados	Indisponibilidade de acesso ao banco de dados. Erro de acesso ao banco de dados. Erro de acesso ao servidor.
Falha no servidor de banco de dados	Erro de acesso ao servidor. Erro de acesso ao banco de dados. Erro de acesso aos dados. Mensagens de erro. Indisponibilidade do servidor.
Falha no servidor ERP	Erro de acesso ao servidor. Erro de acesso ao sistema. Indisponibilidade do servidor.

Riscos	*Impactos*
Falha no sistema ERP	Indisponibilidade de acesso ao sistema. Erro de acesso ao sistema. Erro de acesso ao servidor.

14.7.9.2 Plano de testes

Realizar o *login* no sistema ERP, acionar os recursos do sistema, verificar o uso de CPU e memória.

14.7.9.3 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet.*

14.7.10 Servidor de banco de dados

O que é

É o servidor onde está instalado o gerenciador de banco de dados da empresa.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Banco de dados.
- Servidor de banco de dados.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedor de banco de dados.
- Fornecedores de *software.*

14.7.10.1 Riscos e impactos

A Tabela 102 (Riscos e impactos para o servidor de banco de dados) apresenta a relação de riscos e seus devidos impactos.

Tabela 102: Riscos e impactos para o servidor de banco de dados

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no banco de dados	Indisponibilidade de acesso ao banco de dados. Erro de acesso ao banco de dados. Erro de acesso ao servidor.

Riscos	*Impactos*
Falha no servidor de banco de dados	Erro de acesso ao servidor. Erro de acesso ao banco de dados. Erro de acesso aos dados. Mensagens de erro. Indisponibilidade do servidor.

14.7.10.2 Plano de testes

Realizar testes de acesso ao servidor e ao gerenciador de banco de dados e executar consultas às bases de dados.

14.7.10.3 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet.*

14.7.11 Servidor de arquivos

O que é

É o servidor dedicado ao armazenamento e distribuição de arquivos da M2FE na rede. Também é utilizado para o gerenciamento de *backup* de dados diário da M2FE, recebendo todos os arquivos da rede e copiando os dados para fitas magnéticas.

O que compõe

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Servidor de arquivos.

- *Software* de *backup.*

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.

14.7.11.1 Riscos e impactos

A Tabela 103 (Riscos e impactos para o servidor de arquivos) apresenta a relação de riscos e seus devidos impactos.

Tabela 103: Riscos e impactos para o servidor de arquivos

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no servidor de arquivos	Erro de acesso ao servidor. Erro de acesso aos arquivos. Indisponibilidade dos arquivos. Falha na restauração de arquivos.
Falha no software de *backup*	Indisponibilidade de acesso ao *software.* Erro de acesso ao banco de dados. Erro de acesso ao servidor.

14.7.11.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet.*

14.7.11.3 Plano de testes

Verificação de *logs*.

Verificação de utilização.

Testes mensais de restauração de *backup* em área isolada do disco, isto é, os testes de restauração devem ser realizados em área destinada a testes de restauração.

Testes de conectividade com o servidor.

14.7.12 Servidor de *e-mail*

O que é

É o servidor de sistema de *e-mails* da M2FE.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Servidor de *e-mail.*
- Sistema de *e-mail.*

Fornecedores

- Fornecedor de infraestrutura elétrica.

- Fornecedor de infraestrutura da rede.
- Fornecedor de servidores.
- Fornecedores de *software.*

14.7.12.1 Riscos e impactos

A Tabela 104 (Riscos e impactos para o servidor de e-mail) apresenta a relação de riscos e seus devidos impactos.

Tabela 104: Riscos e impactos para o servidor de e-mail

Riscos	***Impactos***
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica
Falha no servidor de *e-mail*	Erro no sistema de *e-mail.* Indisponibilidade de acesso aos *e-mails.*
Falha no sistema de correio eletrônico	Indisponibilidade de acesso ao sistema. Erro de acesso ao *e-mail.* Erro de acesso ao servidor. Erro na atualização de *e-mails.*

14.7.12.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por telefone ou *Internet*.

14.7.12.3 Plano de testes

Testes de utilização do serviço de *e-mail*.

Testes de memória RAM.

Testes de conectividade com o servidor.

14.7.13 Firewall

O que é

É o servidor que tem por objetivo aplicar regras das políticas de segurança da empresa no acesso à *Internet.* Sua função também consiste em regular o tráfego de dados entre redes distintas e impedir acessos não autorizados de uma rede para outra.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Infraestrutura de *Internet.*
- *Firewall.*

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*
- Fornecedor de servidores.

- Fornecedores de *software.*

14.7.13.1 Riscos e impactos

A Tabela 105 (Riscos e impactos para o *firewall)* apresenta a relação de riscos e seus devidos impactos.

Tabela 105: Riscos e impactos para o *firewall*

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *Firewall*	Indisponibilidade de acesso à *Internet.* Mensagem de erro.

14.7.13.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet*.

14.7.13.3 Plano de testes

Testar acesso à *Internet*.

Testar repasse de pacotes.

Verificar regras de filtragem de pacotes.

Verificar mensagens de erro nos *logs*.

14.7.14 Servidor de *Internet (web)*

O que é

É o servidor *web* da M2FE, que hospeda o *site* institucional da empresa.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Infraestrutura da *Internet.*
- Servidor *Internet web.*

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*

14.7.14.1 Riscos e impactos

A Tabela 106 (Riscos e impactos para o servidor de *Internet* (*web*)) apresenta a relação de riscos e seus devidos impactos.

Tabela 106: Riscos e impactos para o servidor de *Internet* (*web*)

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no servidor de *Internet*	Erro de acesso ao servidor. Erro de acesso às páginas. Indisponibilidade do servidor.

14.7.14.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail*, telefone ou *Internet*.

14.7.14.3 Plano de testes

Testar a acessibilidade do *site* hospedado no servidor.

14.7.15 Servidor *Active Directory*, DHCP e DNS

O que é

É o servidor que implementa o serviço de diretório no protocolo LDAP armazenando informações sobre a rede de computadores e as disponibilizações aos usuários e administradores da rede.

Esse servidor também gerencia nomes, resolve os nomes de servidores em endereços de rede (IP) e oferece a configuração dinâmica de endereços de rede, com concessão de endereços IP de *host* e outros parâmetros de configuração para os clientes da rede.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Servidor *Active Directory*, DHCP e DNS.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*
- Fornecedor de servidores.
- Fornecedores de *software.*

14.7.15.1 Riscos e impactos

A Tabela 107 (Riscos e impactos para o servidor *Active Directory*, DHCP e DNS) apresenta a relação de riscos e seus devidos impactos.

Tabela 107: Riscos e impactos para o servidor *Active Directory*, DHCP e DNS

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no servidor AD, DHCP e DNS	Erro de *login.* Erro de acesso a rede. Erro de acesso aos servidores. Erro de acesso à *Internet.*

14.7.15.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet.*

14.7.15.3 Plano de testes

Testes de autenticação de usuário junto ao servidor *(login)*.

Testes de memória e de uso da CPU.

14.7.16 Roteador de *Internet*

O que é

É o equipamento usado para fazer a conexão da rede corporativa da M2FE com a *Internet*.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Roteador *Internet*.

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.

14.7.16.1 Riscos e impactos

A Tabela 108 (Riscos e impactos para o roteador de *Internet)* apresenta a relação de riscos e seus devidos impactos.

Tabela 108: Riscos e impactos para o roteador de *Internet*

Riscos	*Impactos*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no roteador	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

14.7.16.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet*.

14.7.16.3 Plano de testes

Testar o repasse de pacotes entre a rede local e a *Internet*.

Verificar as ACLs.

Verificar o uso da CPU e da memória.

14.7.17 Proxy

O que é

É o servidor que atua como cachê armazenando páginas da *Internet* visitadas recentemente de forma a aumentar a velocidade de exibição das páginas já visitadas, otimizar o uso do *link* com a *Internet* e controlar o acesso a *sites* não permitidos pela empresa.

O que compõe

Os seguintes componentes encontram-se na M2FE:

- Infraestrutura elétrica.
- Infraestrutura de rede.
- Infraestrutura da *Internet.*
- *Proxy.*

Fornecedores

- Fornecedor de infraestrutura elétrica.
- Fornecedor de infraestrutura da rede.
- Fornecedor de infraestrutura da *Internet.*
- Fornecedor de servidores.
- Fornecedores de *software.*

14.7.17.1 Riscos e impactos

A Tabela 109 (Riscos e impactos para o proxy) apresenta a relação de riscos e seus devidos impactos.

Tabela 109: Riscos e impactos para o *proxy*

Riscos	***Impactos***
Falha na infraestrutura da *Internet*	Erro de acesso à *Internet.* Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

Riscos	*Impactos*
Falha na infraestrutura de rede	Erro de acesso à rede. Mensagem de erro do sistema.
Falha na infraestrutura elétrica	Falta de energia elétrica.
Falha no *proxy*	Mensagem de erro do sistema. Indisponibilidade de acesso à *Internet.*

14.7.17.2 Atendimento

Acionamento da equipe de TI local, através de abertura de chamado, por *e-mail,* telefone ou *Internet*.

14.7.17.3 Plano de testes

Testar o funcionamento do serviço de *proxy*.

Verificar o uso da memória e da CPU.

Verificar mensagens de erro nos *logs*.

Verificar o espaço em disco.

14.7.18 Contatos / Fornecedores

Equipe interna de Suporte TI - M2FE.

- Atendimento em regime de 5 dias por semana por 10 horas (08h00 – 18h00).
- Abertura de chamados via telefone ou *e-mail.*

- Telefone: 0800-123456.
- *e-mail*: suporte@m2fe.com.br.
- Responsável técnico: Gerente de TI.
- Atendimento do chamado em até 1 hora (1º nível).

Fornecedores e Parceiros

Fornecedor de servidores

- Atendimento em regime 7 dias por semana por 24 horas.
- Abertura de chamados via telefone ou *e-mail*
- Telefones de contato: 0800 999 8888.
- Atendimento do chamado em até 4 horas para servidores e 48 horas para microcomputadores.
- Responsável: Gerente Técnico.

Fornecedor de sistema ERP

- Atendimento em regime de 5 dias por semana por 8 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: (19) 3272-9999.
- Atendimento do chamado em até 24 horas.
- Responsável: Gerente Comercial.

Fornecedor de banco de dados

- Atendimento em regime de 5 dias por semana por 8 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: (19) 3272-8888.
- Atendimento do chamado em até 24 horas.
- Responsável: Gerente Técnico.

Fornecedor de *software*

- Atendimento em regime 5 dias por semana por 8 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: (19) 3272-7777.
- Atendimento do chamado em até 24 horas.
- Responsável: Gerente Comercial.

Fornecedores de *link*, roteadores e *switches*

- Atendimento em regime 5 dias por semana por 8 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: (19) 3272-6666.
- Atendimento do chamado em até 24 horas.
- Responsável: Gerente Técnico.

Fornecedor de infraestrutura da *Internet*

- Atendimento em regime 7 dias por semana por 24 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: 0800 999 7777.
- Atendimento do chamado em até 4 horas.
- Responsável: Gerente Técnico.

Fornecedor de infraestrutura da rede

- Atendimento em regime 7 dias por semana por 24 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: 0800 999 6666.
- Atendimento do chamado em até 4 horas.
- Responsável: Gerente Técnico.

Fornecedor de infraestrutura elétrica

- Atendimento em regime 7 dias por semana por 24 horas.
- Abertura de chamados via telefone ou *e-mail.*
- Telefones de contato: 0800 999 5555.
- Atendimento do chamado em até 4 horas.
- Responsável: Gerente Técnico.

14.8 PRD – Plano de Recuperação de Desastres

Quando falamos em desastres, logo nos vem à mente: fogo, inundação e outras causas que provocam danos à propriedade. Mas também consideramos desastres os problemas corriqueiros tais como mau funcionamento de *hardware* ou *software* que necessitam de restauração do seu processamento computacional.

Quando definimos Plano de Recuperação de Desastre como sendo: "*Tem o propósito de definir o plano de restauração e recuperação dos componentes afetados e/ou danificados que suportam os processos de negócio a fim de restabelecer o ambiente e as condições originais de operação.*", devemos também levar em consideração a criticidade do desastre e os níveis de decisões envolvidos em tal evento.

A M2FE está tecnologicamente avançada no mercado e consequentemente é muito dependente da área de TI mediante o uso de computadores, telecomunicações e processamento das informações e qualquer perda prolongada em sua capacidade computacional poderá afetar o seriamente o desempenho em seu negócio.

Caso ocorra um desastre na matriz que afete a sua capacidade computacional, o Comitê do PCN analisará a viabilidade de acionamento do *backup site* e se iniciará o processo do PCN. Caso o desastre não esteja relacionado somente a processos relacionados à área de TI, os procedimentos administrativo-financeiros de pagamento e cobrança deverão ser os primeiros procedimentos a serem implantados no Posto de Comando seguidos dos processos de Engenharia e Aplicação.

14.8.1 Distribuição do Plano

A distribuição do plano é apresentada na Tabela 110 (Distribuição do plano).

Tabela 110: Distribuição do plano

Arquivo Eletrônico	CD-ROM, junto ao posto de comando. Rede Corporativa. *Intranet*.

Papel	Arquivo de controles internos junto a área do CSO, junto ao Posto de Comando.

14.8.2 Descrição Sucinta

Declarada a contingência na M2FE pelo Gestor do PCN:

- Deslocar o pessoal do Grupo de Operações para o Posto de Comando.

14.8.3 Acionamento / Comitê do PCN

O acionamento do comitê de decisão deve ser executado conforme Tabela 111 (Acionamento do Comitê do PCN).

Tabela 111: Acionamento do Comitê do PCN

Responsável pela Ativação	Gerente do Evento - Funcionário3.
Ambiente de Contingência	Escritório Iguatemi.
Prazo da Operação	(4) horas.
Posto do Comando	M2FE – Av. Iguatemi, 1000 – 5º. Andar, salas 50, 51 e 52 Fone 0800-123456

14.8.4 Fluxo de ações

A Tabela 112 (Fluxo de ações) apresenta as prioridades das ações.

Tabela 112: Fluxo de ações

Atividades a serem executadas pelo Comitê do PCN para o nível de alerta primário – Desastre
A - Avaliação inicial da situação
1. Após constatação do nível de alerta primário, os membros do comitê de decisão contatarão os colaboradores, informando aos mesmos o deslocamento para o site de contingência.
2. Entrar em contato com o Gestor do PCN (CSO) para verificar a previsão do tempo de indisponibilidade.
3. Caso o tempo de duração da paralisação seja superior ao admitido para o processo crítico informar o Gestor do PCN (CSO).
4. Comitê do PCN dá início as atividades do PCN – Plano de Continuidade de Negócios .
5. Ativar o site de contingência (Posto de comando).
6. Acionar os colaboradores dos grupos funcionais para o deslocamento para o Posto de Comando.
7. Informar a decisão aos demais colaboradores e informar sobre os procedimentos a serem adotados (aguardar ou dispensar).
8. Orientar o deslocamento dos colaboradores para o Posto de Comando.
9. Contatar os principais clientes (internos e externos) e informar os telefones que serão disponibilizados para contato.
10. Contatar os principais fornecedores interagindo com eles caso seja necessário.
11. Iniciar os trabalhos no *site* de contingência

Atividades a serem executadas pelo Comitê do PCN para o nível de alerta primário – Desastre
12. Monitorar a Situação: ● Membro do Comitê de Decisão mantém contato contínuo com Gestor do PCN para verificar a perspectiva e a estimativa de prazo para a normalização da situação ou liberação do prédio da matriz. ● O Gerente do Evento, após a liberação do prédio, decide se voltará as atividades normais e comunica ao líder da contingência.
13. Após a normalização da Situação: ● Contatar os colaboradores para o retorno ao prédio da matriz da M2FE. ● Realizar os procedimentos básicos para retomada das atividades no prédio da matriz. ● Informar, mediante reunião/relatório, o ocorrido e as soluções adotadas na contingência apresentando sugestões para aprimoramento do plano, enviando-o para Gestor do plano de continuidade de negócios.

14.8.5 Ambiente de contingência - procedimentos imediatos

A Tabela 113 (Restauração do banco de dados) apresenta o procedimento de restauração do banco de dados.

Tabela 113: Restauração do banco de dados

Procedimento:	***Restauração dos sistemas e Banco de Dados***
Atualizar os Servidores e sistemas do *Backup site.*	
Instrução	

01	Restaurar os sistemas aplicativos.
02	Restaurar os bancos de dados.
03	Restaurar os dados do servidor de arquivos .
04	Disponibilizar sistemas para a área Contábil.
05	Disponibilizar sistemas para a área Financeira.

A Tabela 114 (Pagamentos e recebimentos) apresenta o processo de pagamentos e recebimentos.

Tabela 114: Pagamentos e recebimentos

Procedimento:	***Processos de Pagamentos e Recebimentos (fazem parte do Processo de Vendas)***
Atualizar o Sistema Contábil / Financeiro.	
Instrução	
01	Contabilidade: Pode existir atraso contábil de até 5 dias.
02	Contabilidade: Atenção para os casos de vencimento de impostos e entrega de declarações (risco de multas).
03	Receber no Posto de Comando (site de contingência) relatório de cobranças e pagamentos.
04	Ligar para os clientes e fornecedores informando o evento e efetua cobranças/pagamentos.

14.8.6 Infraestrutura Necessária

A Tabela 115 (Infraestrutura) apresenta a infraestrutura necessária.

Tabela 115: Infraestrutura

Serviços Necessários	• Contratação de Transporte. • Suporte para Alimentação. • Contratação de Hospedagem.
Recursos Necessários	• Material de Escritório. • Material para pagamentos e recebimentos (via *Internet* / cheque). • 5 Celulares.
Hardware / Software	• 20 estações. • 3 Impressoras. • 5 telefones. • Sistema ERP (guardar *backup* do banco de dados em local externo à matriz). • MS-Office. • 4 *Notebooks.*
Posto de Comando da M2FE	Av. Iguatemi, 1000 – 5º. Andar, salas 50, 51 e 52 *Help Desk*: Tel: 0800-123456 *E-mail:* helpdesk@m2fe.com.br

14.9 BIA - Business Impact Analysis

BIA (*Business Impact Analysis*) ou Análise de Impacto nos Negócios é um processo de análise utilizado para revelar os impactos empresariais resultantes da paralisação de um processo crítico por um período que exceda o tempo máximo permissível.

A preparação da BIA seguiu os passos descritos a seguir.

Passo 1: Processos

Conhecer detalhadamente os processos de negócio da empresa. Esta etapa foi executada na análise de risco.

Passo 2: Reunião gerencial

Foi apresentada a conceituação da BIA ao corpo gerencial e diretivo da empresa, estabelecendo seus objetivos, prazos e entregáveis.

Foram obtidas as informações do último balanço patrimonial, conforme Tabela 116, e do lucro líquido dos últimos cinco anos, apresentado na Tabela 117 e, gráfico na Figura 62.

Tabela 116: Balanço patrimonial

Ativo (bens e direitos)	*R$*	*Passivo (obrigações)*	*R$*
Bens		**Obrigações**	
Prédio da Matriz	10.000.000,00	Salários	354.000,00
Equipamentos	2.000.000,00	Fornecedores	520.000,00
Benfeitorias	500.000,00	Empréstimos	200.000,00
Ativos diversos	200.000,00	Aluguel - Escritórios	10.000,00
Veículo	250.000,00		
Subtotal Bens	**12.950.000,00**	**Subtotal das obrigações**	**1.084.000,00**
Direitos		**Patrimônio líquido**	

Dinheiro em conta corrente	350.000,00	Capital inicial	15.376.000,00
Dinheiro aplicado	2.000.000,00		
Contas a Receber	1.160.000,00		
Subtotal de direitos	**3.510.000,00**	**Subtotal de patrimônio líquido**	**15.376.000,00**
Total do ativo	**16.460.000,00**	**Total (passivo + patrimônio líquido)**	**16.460.000,00**

Tabela 117: Lucro líquido

Ano	*Lucro líquido (R$)*
2004	150.000,00
2005	720.000,00
2006	1.300.000,00
2007	2.500.000,00
2008	550.000,00

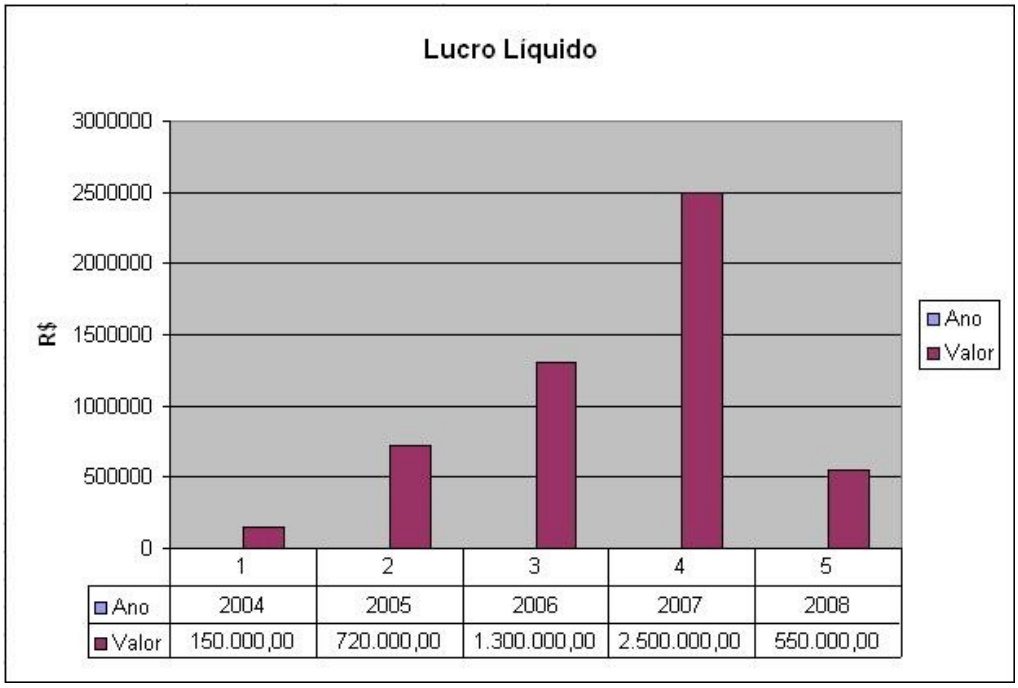


Figura 62: Lucro líquido

É importante ressaltar que o lucro líquido da M2FE foi menor em 2008 devido à ocorrência do incidente de segurança, pois o roubo das informações vitais do projeto da máquina pode ter favorecido a concorrência no lançamento de produtos com as mesmas características.

Passo 3: RTO (*Recovery Time Objective*)

Definir o tempo máximo tolerável, em horas, que um determinado processo pode falhar antes de impactar desastrosamente o negócio. Este tempo é chamado Objetivo de Tempo de Recuperação (RTO - *Recovery Time Objective*).

Cada processo deve ser classificado de acordo com o seu RTO, conforme apresentado na a Tabela 118.

Tabela 118: Classificação do processo segundo seu RTO

Grupo	*RTO permissível (hora)*
1	Menor ou igual a 24 horas.
2	Entre 24 e 48 horas, inclusive.
3	Superior a 48 horas.

Os processos da M2FE possuem os RTOs conforme apresentado na Tabela 119.

Tabela 119: RTOs dos processos da M2FE

Processo	*RTO (h)*	*Grupo*
Formalizar pedido	24	1
Produzir produto	144	3
Contábil, administrativo e financeiro	12	1
Controlar produção	24	1
Aprovar protótipo	72	3
Atender cliente	12	1
Faturar produto	12	1
Controlar produção de campo	72	3
Realizar serviços	12	1
Faturar serviços de campo	72	3
Comprar componentes	24	1

Passo 4: Custo médio diário de cada funcionário

Para obter o custo de cada processo, deve-se determinar as seguintes informações.

- Número de funcionários envolvidos em cada processo.
- Determinar o custo médio diário do funcionário, em Reais, de cada funcionário. Este valor é obtido da coluna Salários do balanço patrimonial, dividido pelo número total de funcionários da empresa para 22 dias úteis. O resultado foi o seguinte:

$$CustoMédioDiário = \frac{TotalSalário}{NúmeroFuncionários * 22}$$

$$CustoMédioDiário = \frac{354000}{70 * 22}$$

$$CustoMédioDiário = 229{,}87$$

Passo 5: Valor de multa diário

Calcula-se o valor da multa diária que, na caso da M2FE, corresponde a 1% do faturamento mensal. O faturamento mensal é determinado a partir da previsão de faturamento anual.

Na M2FE, o valor da multa diária, em Reais, foi calculado da seguinte forma:

$$MultaDiária = (\frac{FaturamentoAnual}{12}) * 0.01$$

$$MultaDiária = (\frac{14000000}{12}) * 0.01$$

$$MultaDiária = 11666{,}67$$

Passo 6: Custo da imagem

Determina-se o custo da imagem, que, no caso da M2FE, foi arbitrado pela diretoria como sendo o valor de R$3000,00 por dia.

Passo 7: Negócio não efetivado

Neste passo, determina-se o valor do negócio que foi impossibilitado de ser efetivado em função do desastre.

No caso da M2FE, este valor foi estimado com base no faturamento mensal, considerando-se que, em média, são fechadas duas vendas de máquinas por mês. Com base nos RTOs, considerou-se que a perda seria de um negócio ao mês, o que representa 50% do faturamento mensal, equivalente a 22 dias úteis.

O processo Formalizar Pedido é o que representa a efetivação do negócio. O valor do negócio não efetivado, em Reais, é o seguinte:

$$NegócioNãoEfetivado = \frac{FaturamentoAnual}{(12 * 2 * 22)}$$

$$NegócioNãoEfetivado = \frac{14000000}{(12 * 2 * 22)}$$

$$NegócioNãoEfetivado = 26515{,}15$$

Passo 8: Custo total por hora de cada processo

Para cada processo, calcula-se o custo total por hora de cada processo da seguinte maneira:

$$TotalHora = \frac{(NF * CMD) + Multa + CI + NE}{24}$$

Onde:

- **NF:** Número de funcionários (70)
- **CMD:** Custo médio diário do funcionário (R$229,87)
- **Multa:** Multa diária (R$11.666,67)
- **CI:** Custo da imagem (R$3.000,00)
- **NE:** Custo do negócio não efetivado

Na M2FE a fórmula foi aplicada a cada processo e os resultados são apresentados na Tabela 120.

Tabela 120: Custo dos processos por hora

Processos	*NF*	*NE (R$)*	*Total Hora (R$)*
Formalizar pedido	3	26.515,15	1.744,64
Produzir produto	8	0,00	687,73
Contábil, administrativo e financeiro	8	0,00	687,73
Controlar produção	5	0,00	659,00
Aprovar protótipo	4	0,00	649,42
Atender cliente	3	0,00	639,84
Faturar produto	2	0,00	630,27
Controlar produção de campo	2	0,00	630,27
Realizar serviços	2	0,00	630,27
Faturar serviços de campo	2	0,00	630,27
Comprar componentes	1	0,00	620,69

Passo 9: Balanço patrimonial depois do desastre

O balanço patrimonial após a ocorrência do desastre é apresentado na Tabela 121.

Tabela 121: Balanço patrimonial após o desastre

Ativo (bens e direitos)	*R$*	*Passivo (obrigações)*	*R$*
Bens		**Obrigações**	
Prédio da Matriz	10.000.000,00	Salários	354.000,00

Equipamentos	2.000.000,00	Fornecedores	520.000,00
Benfeitorias	500.000,00	Empréstimos	200.000,00
Ativos diversos	200.000,00	Aluguel - Escritórios	10.000,00
Veículo	250.000,00	Multa	256.666,67
Subtotal Bens	**12.950.000,00**	**Subtotal das obrigações**	**1.340.666,67**
Direitos		**Patrimônio líquido**	
Dinheiro em conta corrente	350.000,00	Capital inicial	15.376.000,00
Dinheiro aplicado	2.000.000,00	Lucro ou prejuízo acumulado	(256.666,67)
Contas a Receber	1.160.000,00		
Subtotal de direitos	**3.510.000,00**	**Subtotal de patrimônio líquido**	**15.119.333,33**
Total do ativo	**16.460.000,00**	**Total (passivo + patrimônio líquido)**	**16.460.000,00**

A diferença entre o balanço inicial e o balanço após o desastre é o valor da multa, que é calculado da seguinte forma:

$$MultaMensal = Multa * 22$$

Passo 10: Ponto de falência

O ponto de falência ocorre no momento em que o valor total do passivo é igual ao valor total do ativo.

Para determinar o ponto de falência, o primeiro passo é obter a disponibilidade de recursos em caixa (ativo) e a soma das obrigações mensais (passivo).

Os recursos disponíveis em caixa são obtidos da seguinte forma:

$$Caixa = DinheiroEmConta + DinheiroAplicado$$

$$Caixa = 350.000 + 2.000.000$$

$$Caixa = 2.350.000$$

As obrigações mensais são obtidas da seguinte forma:

$$Passivo = Salário + Fornecedores + Empréstimos + Aluguel + Multa$$

$$Passivo = 354.000 + 520.000 + 200.000 + 10.000 + 256.666.67$$

$$Passivo = 1.340.666,67$$

O ponto de falência ocorre quando o valor de todo ativo é consumido pelo valor do passivo, conforme demostrado na Tabela 122.

Tabela 122: Ponto de falência

Mês	***Saldo do ativo***
1	1.009.333,33
2	(331.333,34)
3	(1.672.000,01)
4	(3.012.666,68)
5	(4.353.333,35)
6	(5.694.000,02)
7	(7.034.666,69)

Mês	*Saldo do ativo*
8	(8.375.333,36)
9	(9.716.000,03)
10	(11.056.666,70)
11	(12.397.333,37)
12	(13.738.000,04)
13	(15.078.666,71)
14	(16.419.333,38)
15	(17.760.000,05)

Entre o décimo quarto e décimo quinto meses ocorre a falência, pois o valor do passivo supera o valor do ativo. O gráfico apresentado na Figura 63 ilustra o ponto de falência.

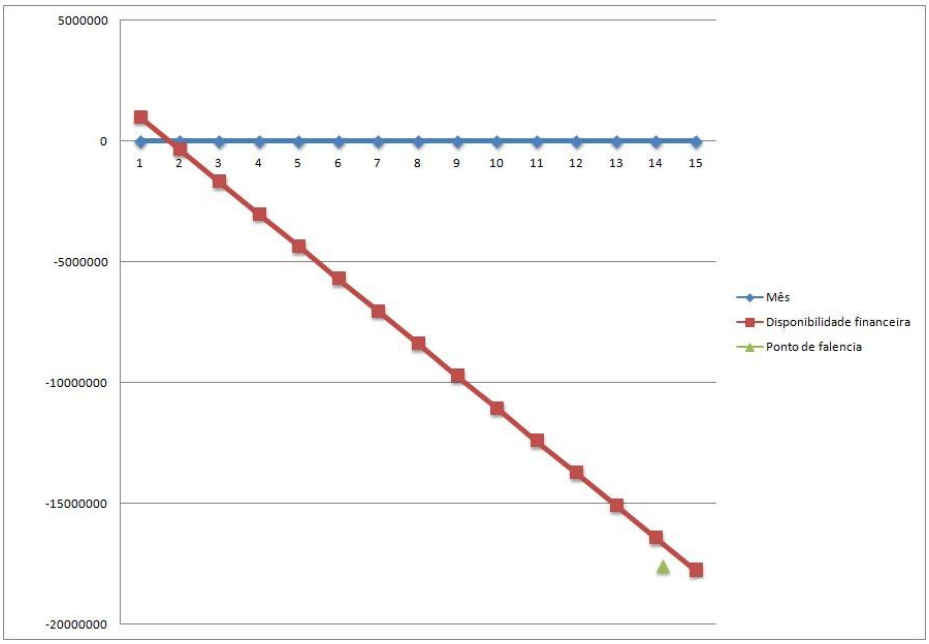


Figura 63: Ponto de falência

O segundo balanço demonstra como direito de receber o item "Contas a Receber" no valor de R$ 1.160.000,00 entretanto, como a empresa não consegue produzir os equipamentos e entregar os serviços o valor real de Conta a Receber é zero (R$ 0,00), sendo

assim a empresa precisa utilizar de suas reservas (Dinheiro aplicado) para pagar suas obrigações.

15 ANÁLISE DE RISCO FINAL

Após o período necessário para a implementação dos controles de segurança, uma nova análise de risco foi executada para a verificação da implementação dos controles e, eventualmente, o levantamento de novos ativos que tenham sido instalados desde a última análise de risco. No caso da M2FE, nenhum novo ativo foi incorporado ao sistema, nem ocorreram alterações nos processos que pudessem exigir um novo levantamento da criticidade dos mesmos ao negócio. Em suma, o ambiente permaneceu o mesmo em termos de ativos e processos e, portanto, nesta nova análise de risco não foram reavaliados os processos, apenas os ativos.

15.1 Firewall

Na primeira análise risco, o *firewall* obteve um índice de conformidade com os controles de pouco mais de 13%. Após a implementação dos controles este cenário modificou-se para melhor, como poderá ser constatado nesta nova análise de risco.

15.1.1 Riscos e controles

Os resultados da aplicação do *checklist* de controles é apresentado na Tabela 123 (*Firewall Netfilter:* controles).

Tabela 123: *Firewall Netfilter*: controles

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Versão do *Netfilter* deve ser a versão estável mais atual	2	TEC	S	1,00	0,00	M	A	-
2	Os registros de *log* do *Netfilter* devem ser analisados diariamente	1	TEC	S	1,00	0,00	M	M	-
3	Os arquivos de *log* devem ser rotacionados semanalmente	2	TEC	S	4,00	0,00	M	M	-
4	O *backup* das regras do *Netfilter* deve ser realizado semanalmente	2	TEC	S	0,00	0,00	B	M	-
5	As regras de filtragem devem ser criadas na ordem correta (e testadas)	8	TEC	N	8,00	0,00	B	A	M
6	O endereço MAC do *gateway* da rede deve ser uma entrada estática na tabela ARP	8	TEC	N	0,50	0,00	M	B	B

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
7	Todas as regras do *Netfilter* devem usar endereços IP e não nomes	8	TEC	S	0,00	0,00	B	M	-
8	As regras antigas devem ser removidas no início da ativação do *Netfilter*	8	TEC	S	0,00	0,00	B	M	-
9	A filtragem de pacotes por estado (SPF) deve ser utilizada nas regras do *Netfilter*	8	TEC	S	0,00	0,00	B	M	-
10	O encaminhamento IP (IP Forward) deve ser desabilitado enquanto as regras do *Netfilter* não tiverem sido carregadas	8	TEC	S	0,50	0,00	M	M	-
11	Permitir tráfego de pacotes ICMP apenas para os tipos 0, 3, 8 e 11 (e*cho reply, destination unreachable, echo request* e *time exceeded*)	8	TEC	S	0,00	0,00	B	B	-

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	As regras do *firewall* (*Netfilter*) devem ser revisadas semestralmente	8	TEC	N	2,00	0,00	M	B	B
13	Apenas tráfego explicitamente autorizado deve ser permitido entre a DMZ e a *intranet*.	1	TEC	S	4,00	0,00	M	A	-
14	Procedimentos de configuração e instalação do *Netfilter* devem estar documentados	2	TEC	N	8,00	0,00	M	B	B
15	Pacotes com *flags* inválidas devem ser bloqueados	2	TEC	N	2,00	0,00	B	M	B
16	Pacotes mal formados devem ser bloqueados pelo *Netfilter*	2	TEC	N	2,00	0,00	M	B	B
17	As regras devem impedir a saída de pacotes da rede interna com IPs públicos	1	TEC	S	1,00	0,00	M	M	-

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	O *firewall Netfilter* deve ser instalado em um computador dedicado	2	TEC	S	0,00	0,00	B	M	-
19	Ferramentas gráficas de gerenciamento do *Netfilter* devem ser removidas	1	TEC	S	0,00	0,00	B	M	-
20	As permissões do arquivo de regras devem ser exclusivas ao usuário root (0600)	2	TEC	N	0,50	0,00	M	B	B
21	As regras do *Netfilter* devem ser elaboradas de forma a registrar em *log* os eventos do tipo *critical.*	2	TEC	S	0,00	0,00	B	M	-
22	As regras mais utilizadas devem ser posicionadas no início da tabela de regras do *Netfilter*	2	TEC	N	1,00	0,00	M	B	B
23	O uso da diretiva *any* nas regras do *Netfilter* deve ser evitado ou minimizado	1	TEC	S	0,50	0,00	M	M	-

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	O conjunto de regras do *Netfilter* deve possuir uma regra que rejeite o tráfego de pacotes do tipo ident	1	TEC	N	0,50	0,00	B	B	B
25	Possui equipamento de reserva?	8	TEC	S	8,00	1500,00	M	A	-

Este ativo utiliza o sistema operacional Linux e os controles de segurança foram implementados, conforme pode ser observado na Tabela 124 (*Firewall Netfilter:* controles do sistema operacional).

Tabela 124: *Firewall Netfilter*: controles do sistema operacional

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Instalar as correções de segurança sempre que disponibilizadas pelo fabricante.	9	TEC	S	5,00	0,00	A	A	-

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
2	Desabilitar os privilégios SUID e SGID dos programas não essenciais à função do servidor.	9	TEC	S	3,00	0,00	A	A	-
3	Desabilitar o serviço *portmap* se o servidor não utilizar NFS.	9	TEC	S	0,50	0,00	M	A	-
4	Limitar o número de processos que um usuário pode executar simultaneamente.	9	TEC	S	0,50	0,00	M	A	-
5	Remover os serviços não necessários para a função do servidor (FTP, DNS, Apache etc).	9	TEC	S	1,50	0,00	M	A	-
6	Desabilitar o acesso da conta root nos consoles locais.	9	TEC	S	0,50	0,00	B	A	-
7	Criar contas com privilégios mínimos para os administradores e adicioná-las no grupo *wheel.*	9	TEC	S	1,00	0,00	M	A	-

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
8	Permitir a elevação de privilégios através do comando su somente ao grupo *wheel.*	9	TEC	S	0,50	0,00	M	A	-
9	Forçar o serviço SSH a aceitar conexões usando apenas a versão 2 do protocolo.	9	TEC	S	0,50	0,00	M	A	-
10	Adicionar apenas as contas dos administradores no grupo *wheel.*	9	TEC	S	0,50	0,00	M	A	-
11	Desabilitar o acesso da conta *root* via SSH.	9	TEC	S	0,50	0,00	M	A	-
12	Remover *banners* de identificação dos serviços habilitados.	9	TEC	S	1,00	0,00	M	M	-
13	Habilitar o registro de acessos de usuários (arquivos *wtmp* e *btmp*).	9	TEC	S	0,50	0,00	B	B	-
14	Habilitar *log* do sistema, separando por tipo de serviço.	9	TEC	S	0,50	0,00	B	B	-

Firewall Netfilter - controles do sistema operacional Linux		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
15	Habilitar o uso do PAM (*Pluggable Authentication Modules*).	9	TEC	S	0,50	0,00	M	M	-
16	Habilitar o *flag* tcp_*syncookies* no TCP/IP para combater ataques do tipo *synflood.*	9	TEC	S	0,50	0,00	M	A	-
17	Desabilitar a resposta a requisições ICMP em *broadcast* (ignore_*broadcasts*=1).	9	TEC	S	0,50	0,00	M	M	-
18	Desabilitar o aceite de pacotes IP roteados pela origem (*.accept_source_route= 0).	9	TEC	S	0,50	0,00	M	M	-
19	Habilitar a verificação de caminho reverso para combater ataques de IP *spoofing* (*rp_filter=1).	9	TEC	S	0,50	0,00	M	M	-
20	Adicionar as opções de montagem nosuid e noexec nas partições de dados (/home, /var etc).	9	TEC	S	0,50	0,00	M	A	-

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
21	Adicionar as opções de montagem nosuid, noexec, nodev à partição /tmp.	9	TEC	S	0,50	0,00	M	M	-
22	Adicionar as opções de montagem nodev, noexec e nosuid às mídias removíveis (fstab).	9	TEC	S	0,50	0,00	B	M	-
23	Ajustar o tempo de ociosidade do console para 5 minutos.	9	TEC	S	0,50	0,00	B	B	-
24	O *layout* de particionamento do disco deve ser adequado (/boot, /, /home, /usr, /var, /tmp etc).	9	TEC	S	0,50	0,00	M	A	-
25	Desabilitar desligamento do computador via CTRL+ALT+DEL.	9	TEC	S	0,50	0,00	B	A	-

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
26	Remover o ambiente gráfico se ele não for estritamente necessário ao funcionamento de alguma aplicação.	9	TEC	S	0,50	0,00	M	A	-
27	Habilitar o registro de eventos de uso do sistema (sysstat - comando sar).	9	TEC	S	0,50	0,00	B	M	-
28	Habilitar o *sticky bit* nos diretórios públicos (/tmp por exemplo).	9	TEC	S	0,50	0,00	M	M	-
29	Remover o suporte aos arquivos .rhosts do PAM.	9	TEC	S	0,50	0,00	M	A	-
30	Restringir o acesso ao agendador de tarefas (*cron* e *at)* apenas aos usuários autorizados.	9	TEC	S	0,50	0,00	B	M	-

Firewall Netfilter - controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
31	Definir e habilitar senha no gerenciador de inicialização (GRUB/Lilo) para restringir o acesso ao modo monousuário.	9	TEC	S	0,50	0,00	B	A	-
32	Garantir que não haja nenhuma conta de usuário ativa com senha nula.	9	TEC	S	0,50	0,00	M	M	-
33	Os diretórios dos usuários (/home) devem possuir atributos 0750 ou mais restritivos.	9	TEC	S	0,50	0,00	M	M	-
34	Ajuste a máscara padrão de criação de arquivos e diretórios para 0770 (não acessíveis globalmente).	9	TEC	S	0,50	0,00	M	M	-
35	Desabilitar a geração de *core dumps* quando programas são abortados.	9	TEC	S	0,50	0,00	B	M	-
36	Desabilitar o *shell* de todas as contas de sistema (serviços).	9	TEC	S	1,00	0,00	M	M	-

15.1.2 Resumo dos riscos

A Tabela 125 (*Firewall Netfilter*: riscos por intensidade) e a Figura 64 resumem a quantidade de riscos a qual o *firewall* está sujeito.

Tabela 125: *Firewall Netfilter*: riscos por intensidade

Firewall *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	1	11,11
B	**Baixo**	8	88,89

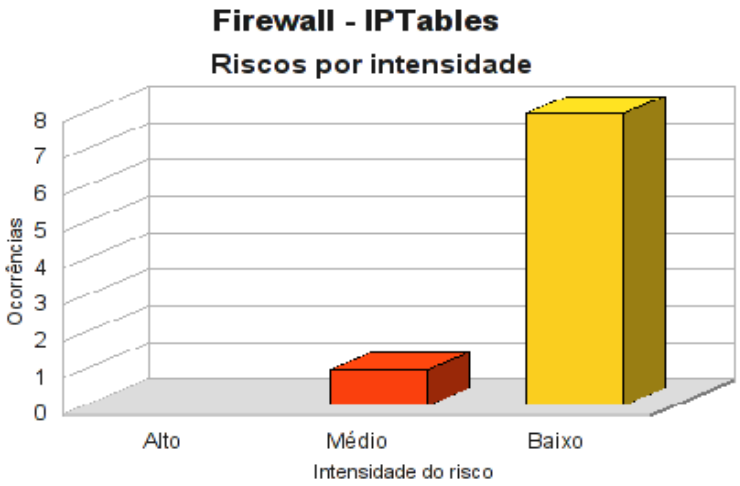


Figura 64: *Firewall Netfilter*: riscos por intensidade

Os riscos identificados para o *firewall* são, na sua totalidade, de características tecnológicas, conforme pode ser observado na Tabela 126 (*Firewall Netfilter:* riscos por tipo de vulnerabilidade) e Figura 65.

Tabela 126: *Firewall Netfilter*: riscos por tipo de vulnerabilidade

Firewall *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	0
M	**Médio**	0	0	1
B	**Baixo**	0	0	8

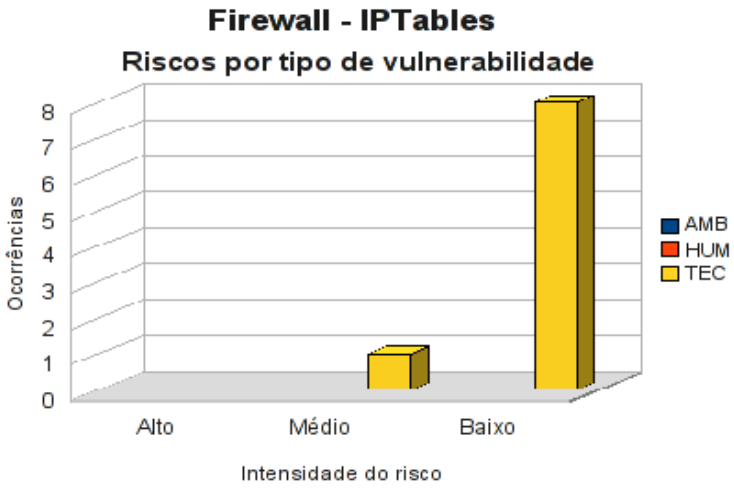


Figura 65: *Firewall Netfilter*: riscos por tipo de vulnerabilidade

15.1.3 Conformidade com os controles

A conformidade com os controles de segurança do *firewall* é apresentada na Tabela 127 (*Firewall Netfilter*: conformidade com os controles) e o gráfico, na Figura 66.

Tabela 127: *Firewall Netfilter*: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	9	14,75
Implementados	52	85,25
Total	**61**	**100,00**

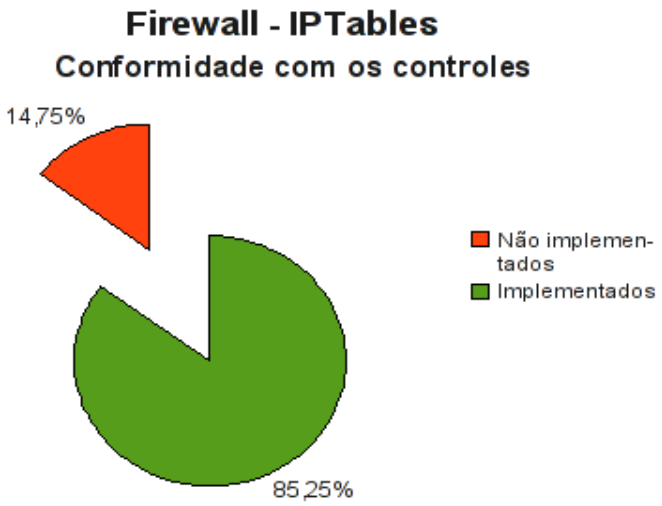


Figura 66: *Firewall Netfilter*: conformidade com os controles

15.1.4 Investimentos necessários

A Tabela 128 (*Firewall Netfilter*: custo estimado para mitigar/controlar os riscos) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *firewall*.

Tabela 128: *Firewall Netfilter*: custo estimado para mitigar/controlar os riscos

Firewall ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	24,50	1715,00
Investimento			0,00
Total a ser investido			**1715,00**

A Tabela 129 (*Firewall Netfilter:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *firewall* por intensidade dos riscos.

Tabela 129: *Firewall Netfilter*: custos por intensidade do risco

Firewall ***Custo estimado para mitigar/controlar os riscos*** ***(por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	560,00
B	**Baixo**	1155,00
Total		**1715,00**

15.2 Servidor de Banco de Dados

O servidor de banco de dados atualmente utilizado é *Oracle* 9i, sendo executado no ambiente operacional *Windows 2003 Server*. Na primeira análise de risco, o índice de conformidade com os controles foi de apenas 12,3%.

15.2.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 130 (Servidor de banco de dados: controles).

Tabela 130: Servidor de banco de dados: controles

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Versão do *software* deve ser a última disponível e compatível com o sistema.	10	TEC	S	40,00	12000,00	A	A	-
2	Aplicar as correções do banco de dados.	2	TEC	S	40,00	0,00	A	A	-
3	A base de dados de desenvolvimento não deve conter dados de produção.	2	HUM	S	8,00	8000,00	A	A	-
4	O servidor deve ser dedicado.	2	TEC	S	8,00	8000,00	M	M	-

Servidor de banco de dados		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
5	Usuários padrões de instalação devem ser removidos ou desabilitados.	1	TEC	S	0,00	0,00	A	A	-
6	Senhas criadas durante a instalação (*default*) devem ser substituídas.	1	TEC	S	4,00	0,00	A	A	-
7	As contas dos usuários SYS e SYSTEM devem ser desabilitadas.	1	TEC	S	0,00	0,00	A	A	-
8	Adotar o princípio de privilégio mínimo para as contas de usuários.	1	TEC	S	0,00	0,00	M	M	-
9	Senhas de conexão ao banco de dados devem estar de acordo com a política.	2	TEC	S	2,00	0,00	M	A	-
10	Remover os privilégios do grupo *PUBLIC*.	2	TEC	S	0,00	0,00	A	M	-
11	Restringir a permissão *ANY* somente ao grupo de administradores.	1	TEC	S	0,00	0,00	A	M	-

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Parâmetro *remote_OS_authentication* em *FALSE.*	1	TEC	N	1,00	0,00	B	B	B
13	Parâmetro *remote_login_passwordfile* em *EXCLUSIVE.*	1	TEC	N	1,00	0,00	B	B	B
14	O *Listener* deve exigir autenticação nas conexões.	9	TEC	S	8,00	0,00	A	M	-
15	Acesso físico ao servidor deve ser restrito e controlado.	6	TEC	S	0,00	0,00	A	A	-
16	Desabilitar ou restringir os dispositivos de armazenamento (fita, CD, USB).	1	TEC	S	2,00	0,00	A	A	-
17	A restauração do banco de dados deve ser restrita e autorizada aos administradores.	1	HUM	S	8,00	0,00	A	A	-
18	Dados armazenados em *backup* devem ser cifrados.	1	TEC	S	40,00	10000,00	M	A	-

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
19	O serviço DBSNMP deve estar desabilitado.	2	TEC	S	0,00	0,00	M	M	-
20	Deve haver procedimento para verificar a liberação de novas correções.	10	TEC	N	8,00	0,00	B	B	B
21	O acesso remoto (*Terminal Service*) deve ser restrito e controlados aos administradores.	1	HUM	S	4,00	0,00	A	M	-
22	O tráfego de dados do banco de dados na rede deve ser cifrado.	2	TEC	S	40,00	0,00	A	A	-
23	Não permitir acesso de analistas aos dados de produção.	11	TEC	S	8,00	0,00	A	A	-
24	Bloquear a execução de DDL para o usuário de conexão da aplicação.	2	TEC	S	0,00	0,00	A	A	-
25	Os arquivos de *trace* só devem ser acessíveis pelo DBA.	11	TEC	S	4,00	0,00	A	A	-

Este ativo utiliza o sistema operacional *Windows 2003 Server* e o *checklist* de controles foi totalmente implementado, conforme demonstrado na Tabela 131 (Servidor de banco de dados: controles do sistema operacional).

Tabela 131: Servidor de banco de dados: controles do sistema operacional

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	S	2,00	0,00	A	A	-
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	S	2,00	0,00	A	A	-
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	S	4,00	0,00	A	A	-
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Remover todos os compartilhamentos não documentados.	2	TEC	S	1,00	0,00	A	A	-
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	S	6,00	0,00	A	A	-
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	S	2,00	0,00	A	A	-
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	S	1,00	0,00	A	A	-
9	Permitir autenticação somente em NTLMv2.	1	TEC	S	1,00	0,00	A	A	-
10	Garantir que a auditoria esteja habilitada.	1	TEC	S	1,00	0,00	A	A	-
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	S	1,00	0,00	A	A	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
12	Desabilitar a conta *guest.*	1	TEC	S	1,00	0,00	A	A	-
13	Renomear a conta do administrador.	1	TEC	S	1,00	0,00	A	A	-
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	S	1,00	0,00	A	A	-
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	S	1,00	0,00	M	M	-
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	S	1,00	0,00	A	A	-
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	S	4,00	0,00	A	A	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	S	1,00	0,00	M	M	-
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	S	8,00	0,00	A	A	-
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	S	1,00	0,00	A	A	-
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	S	1,00	0,00	A	A	-
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	S	2,00	0,00	A	A	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	S	2,00	0,00	A	A	-
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	S	2,00	0,00	A	A	-
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	S	1,00	0,00	A	A	-
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	S	1,00	0,00	A	A	-
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	S	1,00	0,00	B	B	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	S	1,00	0,00	B	B	-
29	Configurar a proteção contra ataques SYN.	9	TEC	S	1,00	0,00	A	A	-
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	S	1,00	0,00	A	A	-
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	S	2,00	0,00	A	A	-
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	S	1,00	0,00	M	M	-
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	S	1,00	0,00	A	A	-
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	S	1,00	0,00	M	M	-

Servidor de banco de dados - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	S	1,00	0,00	A	A	-
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	S	1,00	0,00	M	B	-
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	S	1,00	0,00	A	A	-
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	S	2,00	0,00	A	A	-
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	S	1,00	0,00	A	A	-

15.2.2 Resumo dos riscos

A Tabela 132 (Servidor de banco de dados: riscos por intensidade) e a Figura 67 apresentam o resumo dos riscos o qual o servidor de banco de dados está sujeito.

Tabela 132: Servidor de banco de dados: riscos por intensidade

Servidor de banco de dados *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	0	0,00
B	**Baixo**	3	100,00

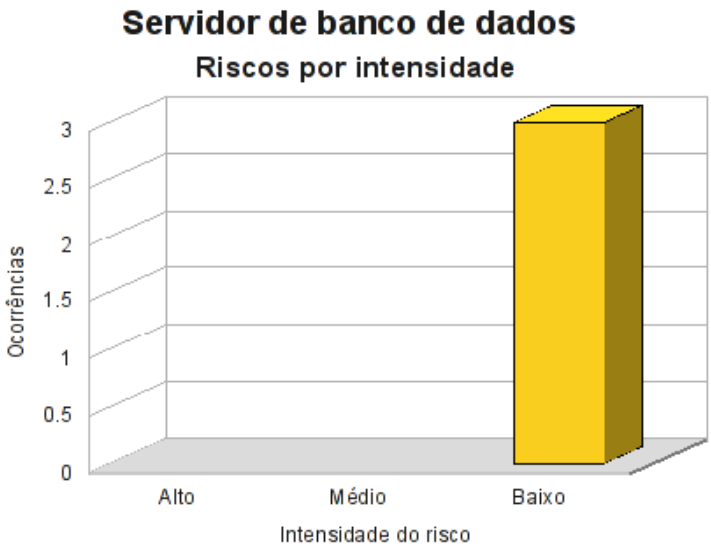


Figura 67: Servidor de banco de dados: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 133 (Servidor de banco de dados: riscos por tipo de vulnerabilidade) e Figura 68.

Tabela 133: Servidor de banco de dados: riscos por tipo de vulnerabilidade

Servidor de banco de dados *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	0	0	0
B	**Baixo**	0	0	3

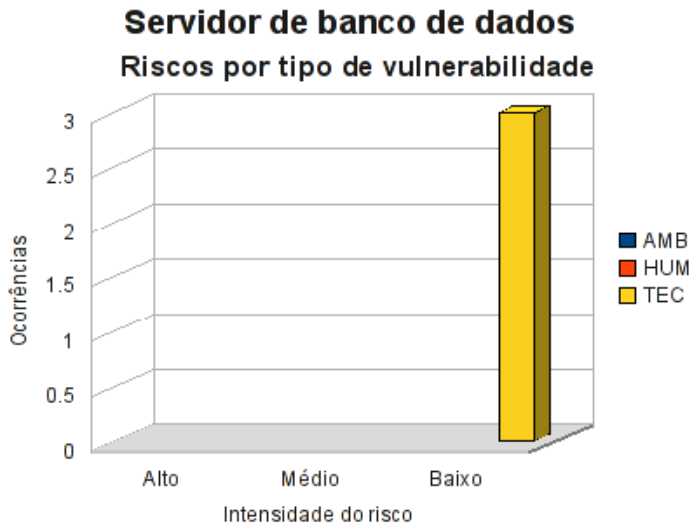


Figura 68: Servidor de banco de dados: riscos por tipo de vulnerabilidade

15.2.3 Conformidade com os controles

A conformidade com os controles de segurança do servidor de banco de dados é apresentada na Tabela 134 (Servidor de banco de dados: conformidade com os controles) e o gráfico, na Figura 69.

Tabela 134: Servidor de banco de dados: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	3	4,62
Implementados	62	95,38
Total	**65**	**100,00**

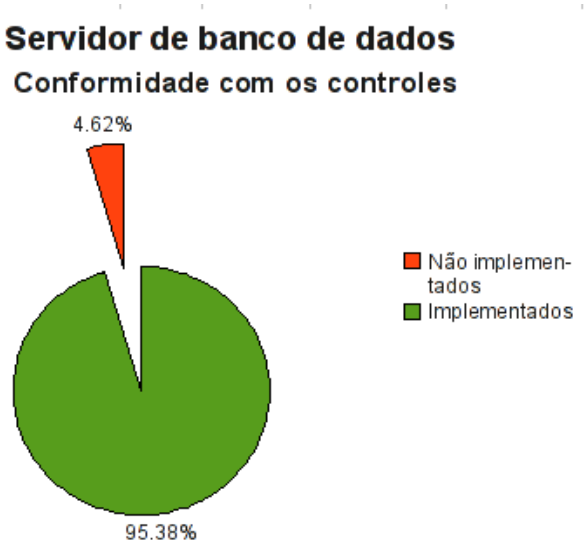


Figura 69: Servidor de banco de dados: conformidade com os controles

15.2.4 Investimentos necessários

A Tabela 135 (Servidor de banco de dados: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor de banco de dados.

Tabela 135: Servidor de banco de dados: custo estimado para mitigar/controlar os riscos

Servidor de banco de dados *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	10,00	700,00
Investimento			0,00
Total a ser investido			**700,00**

A Tabela 136 (Servidor de banco de dados*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor de banco de dados por intensidade dos riscos.

Tabela 136: Servidor de banco de dados: custos por intensidade do risco

Servidor de banco de dados *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	0,00
B	**Baixo**	700,00
Total		**700,00**

15.3 Servidor do sistema ERP

O servidor do sistema de ERP da M2FE contém o sistema que permite a manutenção dos dados cadastrais de funcionários e clientes, além dos dados referentes às compras e vendas efetuadas e a geração de relatórios financeiros e estatísticos. Como nos demais ativos, o índice de conformidade com os controles de segurança do servidor do sistema de ERP encontrado na primeira análise de risco foi baixo: 10,94%.

15.3.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 137 (Servidor ERP: controles).

Tabela 137: Servidor ERP: controles

Servidor ERP		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O banco de dados do ERP não pode ser compartilhado com outras aplicações.	2	HUM	S	32,00	8000,00	M	A	-
2	As senhas não devem ser armazenadas pelo sistema, apenas o *hash* das mesmas.	2	TEC	S	16,00	0,00	A	A	-
3	Todos os arquivos da aplicação ou criados pela mesma devem estar protegidos de acessos não autorizados.	2	TEC	S	80,00	0,00	A	M	-

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	As mudanças devem ser analisadas e aprovadas antes da sua implementação.	11	HUM	S	0,00	0,00	A	A	-
5	Documentar os controles de segurança, responsabilidades e procedimentos.	11	HUM	N	240,00	0,00	M	M	M
6	O controle de acesso da aplicação deve ser baseado em segregação de funções.	2	TEC	S	24,00	0,00	M	A	-
7	Somente os responsáveis pela segurança poderão liberar acesso aos usuários.	11	HUM	S	0,00	0,00	M	M	-
8	O acesso à informação, bens e recursos devem ser restritos somente aos usuários autorizados.	2	TEC	S	0,00	0,00	M	M	-
9	As contas de usuários inativos devem ser desabilitadas.	2	TEC	N	16,00	0,00	M	B	B

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	Os procedimentos de atualização de *software* devem estar documentados.	11	HUM	N	24,00	0,00	B	B	B
11	Garantir que os desenvolvedores não tenham acesso ao ambiente de produção.	11	TEC	N	8,00	8000,00	B	A	M
12	Todas as ações dos usuários devem ser registradas em *log* (trilha de auditoria).	1	TEC	N	8,00	0,00	B	M	B
13	As contas de usuários devem ser desativadas após 3 tentativas consecutivas de acesso sem sucesso.	1	TEC	S	8,00	0,00	A	A	-
14	Adotar o princípio de privilégio mínimo para as contas de usuário.	1	TEC	S	0,00	0,00	M	M	-
15	A comunicação entre a aplicação e o banco de dados deve ser cifrada.	2	TEC	S	40,00	0,00	M	A	-

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
16	O código da aplicação não deve ser mantido junto com a aplicação.	11	HUM	S	8,00	0,00	A	A	-
17	Os recursos de rede (IP, URL etc), chaves e senhas não podem ser *hardcoded.*	11	HUM	S	0,00	0,00	A	A	-
18	Os arquivos de *log* devem ser rotacionados semanalmente.	8	TEC	S	4,00	0,00	M	M	-
19	As atividades dos administradores devem ser registradas em *log* e monitoradas.	8	TEC	S	16,00	0,00	B	A	-
20	Deve ser emitido aviso quando os *logs* estiverem a 80% da capacidade de saturação.	1	TEC	N	8,00	0,00	B	B	B
21	Qualquer ferramenta de auditoria devem ser de uso restrito aos auditores.	2	TEC	S	0,00	0,00	B	M	-

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
22	Verificar semestralmente se os *user IDs* são válidos, aprovados e com segregação de funções (auditoria).	11	HUM	S	16,00	0,00	M	A	-
23	Nenhuma conexão anônima deve ser permitida pela aplicação.	9	TEC	S	0,00	0,00	A	A	-
24	Revisar semestralmente as regras de acesso para garantir que nenhuma regra tenha sido alterada.	11	HUM	N	16,00	0,00	B	M	B

Este ativo utiliza o sistema operacional *Windows 2003 Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 138 (Servidor ERP: controles do sistema operacional).

Tabela 138: Servidor ERP: controles do sistema operacional

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	S	2,00	0,00	A	A	-
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	S	2,00	0,00	A	A	-
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	S	4,00	0,00	A	A	-
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
5	Remover todos os compartilhamentos não documentados.	2	TEC	S	1,00	0,00	A	A	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	S	6,00	0,00	A	A	-
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	S	2,00	0,00	A	A	-
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	S	1,00	0,00	A	A	-
9	Permitir autenticação somente em NTLMv2.	1	TEC	S	1,00	0,00	A	A	-
10	Garantir que a auditoria esteja habilitada.	1	TEC	S	1,00	0,00	A	A	-
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	S	1,00	0,00	A	A	-
12	Desabilitar a conta *guest.*	1	TEC	S	1,00	0,00	A	A	-
13	Renomear a conta do administrador.	1	TEC	S	1,00	0,00	A	A	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	S	1,00	0,00	A	A	-
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	S	1,00	0,00	M	M	-
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	S	1,00	0,00	A	A	-
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	S	4,00	0,00	A	A	-
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC	S	1,00	0,00	M	M	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	S	8,00	0,00	A	A	-
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	S	1,00	0,00	A	A	-
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	S	1,00	0,00	A	A	-
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	S	2,00	0,00	A	A	-
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	S	2,00	0,00	A	A	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	S	2,00	0,00	A	A	-
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	S	1,00	0,00	A	A	-
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	S	1,00	0,00	A	A	-
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	S	1,00	0,00	B	B	-
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	S	1,00	0,00	B	B	-
29	Configurar a proteção contra ataques SYN.	9	TEC	S	1,00	0,00	A	A	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	S	1,00	0,00	A	A	-
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	S	2,00	0,00	A	A	-
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports.*	1	TEC	S	1,00	0,00	M	M	-
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	S	1,00	0,00	A	A	-
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	S	1,00	0,00	M	M	-
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	S	1,00	0,00	A	A	-
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	S	1,00	0,00	M	B	-

Servidor ERP - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	S	1,00	0,00	A	A	-
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	S	2,00	0,00	A	A	-
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	S	1,00	0,00	A	A	-

15.3.2 Resumo dos riscos

A Tabela 139 (Servidor ERP: riscos por intensidade) e a Figura 70 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 139: Servidor ERP: riscos por intensidade

Servidor ERP *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	2	28,57
B	**Baixo**	5	71,43

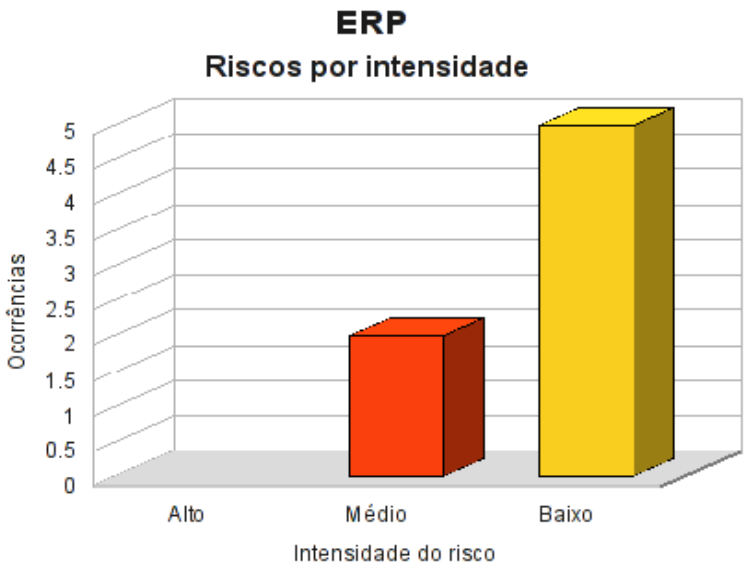


Figura 70: Servidor ERP: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 140 (Servidor ERP: riscos por tipo de vulnerabilidade) e Figura 71.

Tabela 140: Servidor ERP: riscos por tipo de vulnerabilidade

Servidor ERP *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	0	1	1
B	**Baixo**	0	2	3

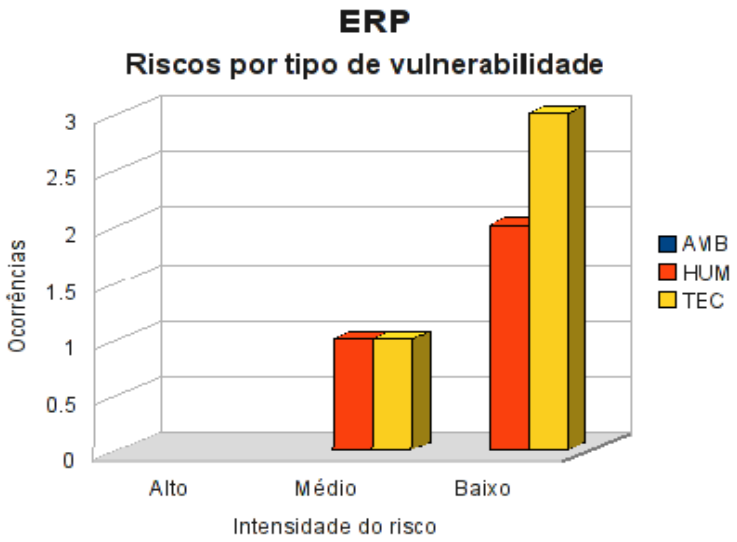


Figura 71: Servidor ERP: riscos por tipo de vulnerabilidade

15.3.3 Conformidade com os controles

A conformidade com os controles de segurança do servidor ERP é apresentada na Tabela 141 (Servidor ERP: conformidade com os controles) e o gráfico, na Figura 72.

Tabela 141: Servidor ERP: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	7	10,94
Implementados	57	89,06
Total	**64**	**100,00**

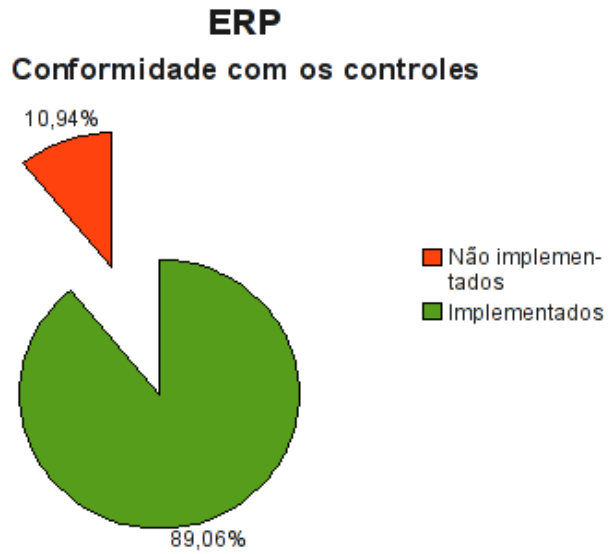


Figura 72: Servidor ERP: conformidade com os controles

15.3.4 Investimentos necessários

A Tabela 142 (Servidor ERP: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor ERP.

Tabela 142: Servidor ERP: custo estimado para mitigar/controlar os riscos

Servidor ERP *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	320,00	22400,00
Investimento			8000,00
Total a ser investido			**30400,00**

A Tabela 143 (Servidor ERP*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no servidor ERP por intensidade dos riscos.

Tabela 143: Servidor ERP: custos por intensidade do risco

Servidor ERP *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	25360,00
B	**Baixo**	5040,00
Total		**30400,00**

15.4 Servidor Windows Active Directory

Na primeira análise de risco, o servidor *Windows Active Directory* obteve apenas 11,86% de conformidade com os controles de segurança.

15.4.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 144 (*Windows Active Directory*: controles).

Tabela 144: *Windows Active Directory*: controles

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Habilitar complexidade de senhas na política de domínio conforme a política da empresa.	1	TEC	S	0,00	0,00	A	A	-
2	Habilitar política de histórico das últimas 5 senhas na política de domínio.	1	TEC	S	1,00	0,00	A	A	-
3	Habilitar o requisito mínimo de 8 caracteres para todas as senhas das contas dos domínios.	1	TEC	S	0,00	0,00	A	A	-

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	Habilitar o requisito minimo de 15 caracteres para todas as contas administrativas.	1	TEC	S	1,00	0,00	A	A	-
5	Restringir o acesso remoto aos servidores Controladores de Domínio aos administradores.	1	TEC	S	1,00	0,00	A	A	-
6	Documentar todos servidores *Active Directory* e Global *catalog*.	2	TEC	S	8,00	0,00	A	A	-
7	Documentar o FSMO (regras do domínio).	2	TEC	S	2,00	0,00	A	A	-
8	Garantir que todos os A*ctive Directories* estão sincronizados.	10	TEC	S	0,00	0,00	A	A	-
9	Proteger o acesso ao *Active Directory Schema Master* de acesso não autorizado.	1	TEC	S	0,00	0,00	A	A	-

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	Possuir pelo menos 2 servidores controladores de domínio trabalhando ativamente.	10	TEC	S	8,00	5000,00	A	A	-
11	Garantir que os servidores de *Active Directory* são dedicados para esta função.	10	TEC	S	0,00	0,00	A	A	-
12	As contas de serviço devem possuir nomes longos, com alta complexidade de senhas e não podem expirar.	1	TEC	S	2,00	0,00	A	A	-
13	Garantir que os administradores possuem contas separadas para as atividades diárias e outra para as administrativas.	2	TEC	S	1,00	0,00	A	A	-
14	Executar diariamente o *backup* da SAM e do *Schema Master*.	2	TEC	S	1,00	0,00	A	A	-

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
15	Utilizar o serviço de DNS integrado ao *Active Directory* apenas para *hosts* internos (do domínio).	10	TEC	S	0,00	0,00	A	A	-
16	Possuir ao menos 2 servidores habilitados com *Global Catalog* na Floresta.	10	TEC	S	1,00	0,00	A	A	-
17	Utilizar serviço NTP para sincronização de data e hora para todos os servidores.	10	TEC	S	2,00	0,00	A	A	-
18	Documentar procedimento de promoção e remoção de controladores de domínios.	11	TEC	S	0,00	0,00	A	A	-
19	Garantir que todas as atualizações de segurança sejam instaladas.	1	TEC	S	1,00	0,00	A	A	-

Este ativo utiliza o sistema operacional *Windows 2003 Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 145 (*Windows Active Directory*: controles do sistema operacional).

Tabela 145: *Windows Active Directory*: controles do sistema operacional

Windows Active Directory - controles do sistema operacional Windows 2003 Server		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	S	2,00	0,00	A	A	-
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	S	2,00	0,00	A	A	-
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	S	4,00	0,00	A	A	-
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Remover todos os compartilhamentos não documentados.	2	TEC	S	1,00	0,00	A	A	-
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	S	6,00	0,00	A	A	-
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	S	2,00	0,00	A	A	-
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	S	1,00	0,00	A	A	-
9	Permitir autenticação somente em NTLMv2.	1	TEC	S	1,00	0,00	A	A	-
10	Garantir que a auditoria esteja habilitada.	1	TEC	S	1,00	0,00	A	A	-
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	S	1,00	0,00	A	A	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
12	Desabilitar a conta *guest.*	1	TEC	S	1,00	0,00	A	A	-
13	Renomear a conta do administrador.	1	TEC	S	1,00	0,00	A	A	-
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	S	1,00	0,00	A	A	-
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	S	1,00	0,00	M	M	-
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	S	1,00	0,00	A	A	-
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	S	4,00	0,00	A	A	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Desabilitar o *autorun* de todos os *drives.*	2	TEC	S	1,00	0,00	M	M	-
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	S	8,00	0,00	A	A	-
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	S	1,00	0,00	A	A	-
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	S	1,00	0,00	A	A	-
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	S	2,00	0,00	A	A	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	S	2,00	0,00	A	A	-
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	S	2,00	0,00	A	A	-
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	S	1,00	0,00	A	A	-
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	S	1,00	0,00	A	A	-
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	S	1,00	0,00	B	B	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	S	1,00	0,00	B	B	-
29	Configurar a proteção contra ataques SYN.	9	TEC	S	1,00	0,00	A	A	-
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	S	1,00	0,00	A	A	-
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	S	2,00	0,00	A	A	-
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	S	1,00	0,00	M	M	-
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	S	1,00	0,00	A	A	-
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	S	1,00	0,00	M	M	-

Windows Active Directory - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	S	1,00	0,00	A	A	-
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	S	1,00	0,00	M	B	-
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	S	1,00	0,00	A	A	-
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	S	2,00	0,00	A	A	-
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	S	1,00	0,00	A	A	-

15.4.2 Resumo dos riscos

A Tabela 146 (*Windows Active Directory*: riscos por intensidade) apresenta o resumo dos riscos aos quais este ativo está sujeito.

Tabela 146: *Windows Active Directory*: riscos por intensidade

Windows Active Directory ***Resumo dos riscos por intensidade***			
Nível		***Ocorrências***	***%***
A	**Alto**	0	0,00
M	**Médio**	0	0,00
B	**Baixo**	0	0,00

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 147 (*Windows Active Directory*: riscos por tipo de vulnerabilidade).

Tabela 147: *Windows Active Directory*: riscos por tipo de vulnerabilidade

Windows Active Directory ***Resumo dos riscos por tipo de vulnerabilidade***				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	0
M	**Médio**	0	0	0
B	**Baixo**	0	0	0

15.4.3 Conformidade com os controles

A conformidade com os controles de segurança do *Windows Active Directory* é apresentada na Tabela 148 (*Windows Active Directory*: conformidade com os controles).

Tabela 148: *Windows Active Directory*: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	0	0,00
Implementados	59	100,00
Total	**59**	**100,00**

15.4.4 Investimentos necessários

A Tabela 149 (*Windows Active Directory*: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Windows Active Directory*.

Tabela 149: *Windows Active Directory*: custo estimado para mitigar/controlar os riscos

Windows Active Directory ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	0,00	0,00
Investimento			0,00
Total a ser investido			**0,00**

A Tabela 150 (*Windows Active Directory:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Windows Active Directory* por intensidade dos riscos.

Tabela 150: *Windows Active Directory*: custos por intensidade do risco

Windows Active Directory ***Custo estimado para mitigar/controlar os riscos*** ***(por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	0,00
B	**Baixo**	0,00
Total		**0,00**

15.5 Servidor de arquivos

Na primeira análise de risco, o servidor de arquivos possuía apenas 10,17% dos controles de segurança implementados.

15.5.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 151 (Servidor de arquivos: controles).

Tabela 151: Servidor de arquivos: controles

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Todos os compartilhamentos devem ser documentados.	2	TEC	S	8,00	0,00	M	M	-
2	Todos os compartilhamentos devem ser ocultos.	1	TEC	S	2,00	0,00	M	M	-
3	O mapeamento dos compartilhamentos deve ser feito via GPO.	2	TEC	S	0,00	0,00	B	B	-
4	Garantir que o IIS não esteja instalado no servidor.	2	TEC	S	0,00	0,00	A	A	-
5	A estrutura de pastas deve seguir o organograma da empresa.	2	TEC	S	0,00	0,00	A	A	-
6	O diretório *home* de cada usuário deve ter acesso restrito ao usuário proprietário do diretório.	2	TEC	N	8,00	0,00	M	M	M

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
7	Deve ser configurado uma quota de 1GB por usuário.	10	TEC	S	0,00	0,00	A	A	-
8	O conteúdo do diretório público da rede deve ser apagado diariamente às 00h00.	2	TEC	S	1,00	0,00	M	M	-
9	Documentar todas as unidades mapeadas, conforme sua função.	2	TEC	S	2,00	0,00	A	A	-
10	Deve ser fornecida área cifrada para armazenamento de arquivos classificados como confidenciais.	2	TEC	S	8,00	0,00	A	A	-
11	Garantir que o grupo *everyone* (todos) seja removido de todos os compartilhamentos.	2	TEC	S	2,00	0,00	A	A	-
12	Garantir que esteja sendo cumprida a política de *backup.*	2	TEC	S	1,00	0,00	A	A	-

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
13	Garantir que os arquivos compartilhados estejam em uma partição diferente da utilizada pelo sistema operacional.	2	TEC	S	0,00	0,00	A	A	-
14	Garantir que este servidor seja exclusivo para compartilhamento de arquivos.	10	TEC	S	0,00	0,00	A	A	-
15	Garantir que todos os arquivos de trabalho sejam gravados no servidor.	2	TEC	S	4,00	0,00	A	A	-
16	Habilitar o recurso de *Shadow Copies* no volume onde os compartilhamentos estão criados.	2	TEC	S	2,00	0,00	M	M	-
17	Configurar o *Shadow Copies* para executar todos os dias da semana às 10h00 e às 15h00.	2	TEC	S	1,00	0,00	M	M	-

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Limitar o tamanho do *Shadow copies* para 20GB.	2	TEC	S	1,00	0,00	A	A	-
19	Auditar bimestralmente a conformidade de permissões com as definidas pela diretoria.	2	TEC	S	1,00	0,00	A	A	-

Este ativo utiliza o sistema operacional *Windows* 2003 *Server* e o resultado da aplicação do *checklist* de controles para este sistema operacional é apresentado na Tabela 152 (Servidor de arquivos: controles do sistema operacional).

Tabela 152: Servidor de arquivos: controles do sistema operacional

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC	S	2,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC	S	2,00	0,00	A	A	-
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC	S	4,00	0,00	A	A	-
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
5	Remover todos os compartilhamentos não documentados.	2	TEC	S	1,00	0,00	A	A	-
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC	S	6,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC	S	2,00	0,00	A	A	-
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC	S	1,00	0,00	A	A	-
9	Permitir autenticação somente em NTLMv2.	1	TEC	S	1,00	0,00	A	A	-
10	Garantir que a auditoria esteja habilitada.	1	TEC	S	1,00	0,00	A	A	-
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC	S	1,00	0,00	A	A	-
12	Desabilitar a conta *guest.*	1	TEC	S	1,00	0,00	A	A	-
13	Renomear a conta do administrador.	1	TEC	S	1,00	0,00	A	A	-
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC	S	1,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID*.	2	TEC	S	1,00	0,00	M	M	-
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC	S	1,00	0,00	A	A	-
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC	S	4,00	0,00	A	A	-
18	Desabilitar o *autorun* de todos os *drives.*	2	TEC	S	1,00	0,00	M	M	-
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC	S	8,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC	S	1,00	0,00	A	A	-
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC	S	1,00	0,00	A	A	-
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC	S	2,00	0,00	A	A	-
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC	S	2,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC	S	2,00	0,00	A	A	-
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC	S	1,00	0,00	A	A	-
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC	S	1,00	0,00	A	A	-
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC	S	1,00	0,00	B	B	-
28	Garantir que as configurações de rede estejam documentadas.	11	TEC	S	1,00	0,00	B	B	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
29	Configurar a proteção contra ataques SYN.	9	TEC	S	1,00	0,00	A	A	-
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC	S	1,00	0,00	A	A	-
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC	S	2,00	0,00	A	A	-
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC	S	1,00	0,00	M	M	-
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC	S	1,00	0,00	A	A	-
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC	S	1,00	0,00	M	M	-
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC	S	1,00	0,00	A	A	-

Servidor de arquivos - controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC	S	1,00	0,00	M	B	-
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC	S	1,00	0,00	A	A	-
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC	S	1,00	0,00	A	A	-
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC	S	2,00	0,00	A	A	-
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC	S	1,00	0,00	A	A	-

15.5.2 Resumo dos riscos

A Tabela 153 (Servidor de arquivos: riscos por intensidade) e a Figura 73 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 153: Servidor de arquivos: riscos por intensidade

Servidor de arquivos *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	1	100,00
B	**Baixo**	0	0,00

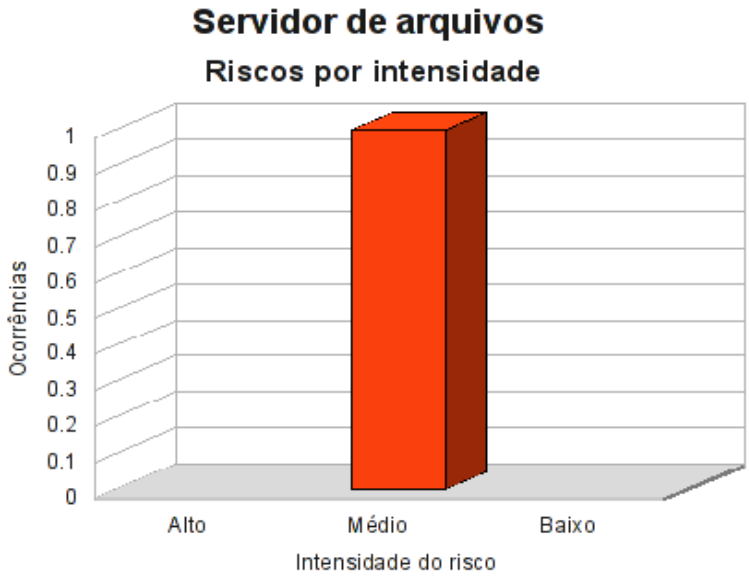


Figura 73: Servidor de arquivos: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 154 (Servidor de arquivos: riscos por tipo de vulnerabilidade) e na Figura 74.

Tabela 154: Servidor de arquivos: riscos por tipo de vulnerabilidade

Servidor de arquivos *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	0	0	1
B	**Baixo**	0	0	0

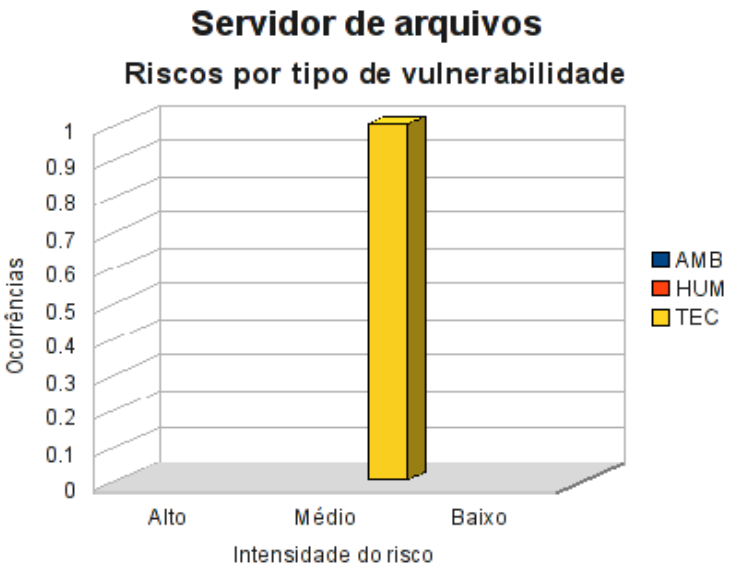


Figura 74: Servidor de arquivos: riscos por tipo de vulnerabilidade

15.5.3 Conformidade com os controles

A conformidade com os controles de segurança do Servidor de arquivos é apresentada na Tabela 155 (Servidor de arquivos: conformidade com os controles) e o gráfico, na Figura 75.

Tabela 155: Servidor de arquivos: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	1	1,69
Implementados	58	98,31
Total	**59**	**100,00**

Figura 75: Servidor de arquivos: conformidade com os controles

15.5.4 Investimentos necessários

A Tabela 156 (Servidor de arquivos: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no Servidor de arquivos.

Tabela 156: Servidor de arquivos: custo estimado para mitigar/controlar os riscos

Servidor de arquivos *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total***
Custo estimado	70,00	8,00	560,00
Investimento			0,00
Total a ser investido			**560,00**

A Tabela 157 (Servidor de arquivos*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no Servidor de arquivos por intensidade dos riscos.

Tabela 157: Servidor de arquivos: custos por intensidade do risco

Servidor de arquivos *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	560,00
B	**Baixo**	0,00
Total		**560,00**

15.6 Data center

Na primeira análise de risco, o *data center* encontrava-se com 33,33% dos controles implementados.

15.6.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 158 (*Data center*: controles).

Tabela 158: *Data center*: controles

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Remover do interior do *data center* todos os materiais não relacionados às atividades do mesmo.	11	HUM	S	8,00	0,00	M	M	-
2	Instalar filtros de limpeza ou contra gases e vapores.	7	TEC	N	16,00	1000,00	M	M	M
3	Deve existir um termostato exclusivo para controle de temperatura do *data center*.	10	TEC	S	0,00	0,00	M	M	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	Deve ser definido e instalado um sistema de refrigeração de contingência para o *data center*.	4	TEC	S	40,00	5000,00	A	A	-
5	O sistema de refrigeração do *data center* deve ser exclusivo.	4	TEC	S	0,00	0,00	M	M	-
6	Devem ser elaborados registros de manutenção preventiva do sistema de ar condicionado.	4	TEC	S	0,00	0,00	A	M	-
7	Instalar câmeras de CFTV externas e internas ao *data center* e armazenar as imagens por 180 dias.	1	TEC	N	16,00	1000,00	M	M	M
8	Não permitir o acesso de visitantes ao *data center* sem prévia autorização da segurança e sem acompanhante.	1	HUM	S	0,00	0,00	A	A	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
9	A porta do *data center* deve ser provida de mecanismo de fechamento automático.	1	TEC	N	8,00	2000,00	M	M	M
10	Os circuitos elétricos do *data center* devem ser divididos e dimensionados adequadamente.	10	TEC	S	0,00	0,00	A	A	-
11	Devem ser instalados circuitos elétricos com tomadas suficientes para o *data center*.	8	TEC	S	0,00	0,00	A	M	-
12	Devem ser instaladas pelo menos duas unidades de luz de emergência no interior do *data center*.	8	TEC	S	0,00	0,00	M	B	-
13	A tensão de alimentação dos equipamentos do *data center* deve ser estabilizada.	8	TEC	S	0,00	0,00	A	M	-

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	Devem ser instalados *no-breaks* para os equipamentos críticos do *data center*.	8	TEC	S	0,00	0,00	A	A	-
15	Não deve haver nenhuma identificação da localização do *data center*.	1	HUM	S	0,00	0,00	B	B	-

15.6.2 Resumo dos riscos

A Tabela 159 (*Data center*: riscos por intensidade) e a Figura 76 apresentam o resumo dos riscos aos quais este ativo está sujeito.

Tabela 159: *Data center*: riscos por intensidade

Data center *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	3	100,00
B	**Baixo**	0	0,00

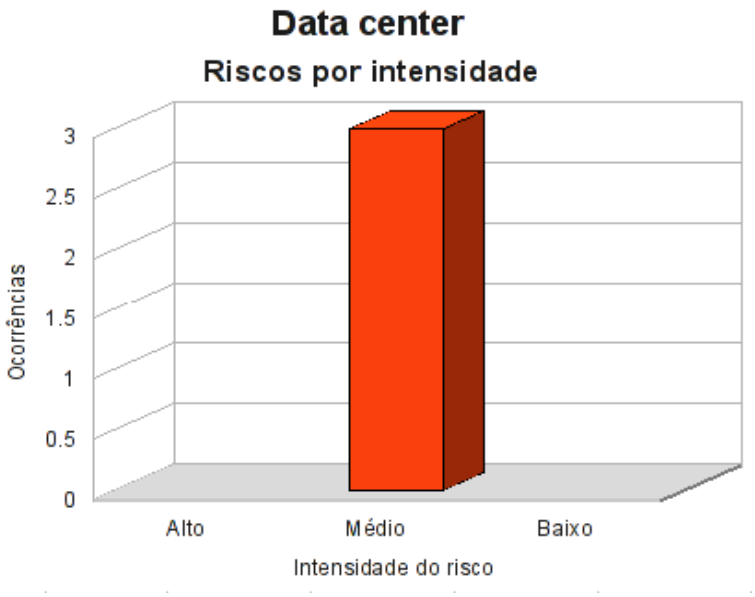


Figura 76: *Data center*: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 160 (*Data center*: riscos por tipo de vulnerabilidade) e na Figura 77.

Tabela 160: *Data center*: riscos por tipo de vulnerabilidade

Data center ***Resumo dos riscos por tipo de vulnerabilidade***				
Risco		***Ocorrências***		
		AMB	***HUM***	***TEC***
A	**Alto**	0	0	0
M	**Médio**	0	0	3
B	**Baixo**	0	0	0

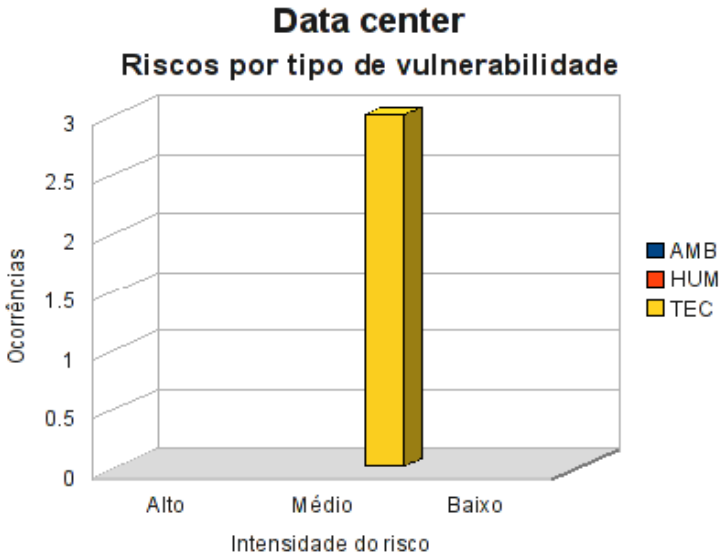


Figura 77: *Data center*: riscos por tipo de vulnerabilidade

15.6.3 Conformidade com os controles

A conformidade com os controles de segurança do *Data center* é apresentada na Tabela 161 e o gráfico, na Figura 78.

Tabela 161: *Data center*: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	3	20,00
Implementados	12	80,00
Total	**15**	**100,00**

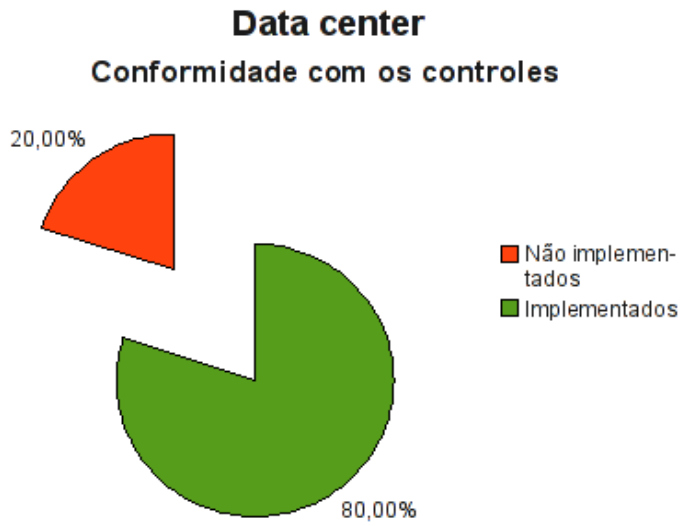


Figura 78: *Data center*: conformidade com os controles

15.6.4 Investimentos necessários

A Tabela 162 (*Data center*: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Data center*.

Tabela 162: *Data center*: custo estimado para mitigar/controlar os riscos

Data center ***Custo estimado para mitigar/controlar os riscos***			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	40,00	2800,00
Investimento			4000,00
Total a ser investido			**6800,00**

A Tabela 163 (*Data center:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados no *Data center* por intensidade dos riscos.

Tabela 163: *Data center*: custos por intensidade do risco

Data center ***Custo estimado para mitigar/controlar os riscos (por intensidade do risco)***		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	6800,00
B	**Baixo**	0,00
Total		**6800,00**

15.7 Análise da rede

Na primeira análise de risco, a rede possuía 35,14% dos controles de segurança implementados.

15.7.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 164 (Rede: controles).

Tabela 164: Rede: controles

Rede		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O endereçamento IP utilizado na LAN é privado (RFC1918).	8	TEC	S	0,00	0,00	B	B	-
2	O cabeamento de rede é certificado.	8	TEC	S	0,00	0,00	B	B	-
3	Devem ser utilizadas fibras ópticas com redundância entre os *switches* de distribuição e o *Core.*	8	TEC	S	0,00	0,00	B	B	-
4	A topologia da rede deve ser estruturada em formato *full mesh* (redundância).	8	TEC	N	8,00	2000,00	B	M	B
5	O protocolo STP deve estar habilitado e configurado corretamente.	8	TEC	N	4,00	0,00	B	M	B
6	A rede deve ser segmentada.	8	TEC	S	80,00	0,00	M	A	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
7	Deve ser utilizado *switch core* L3 com redundância.	8	TEC	N	8,00	10000,00	B	A	M
8	Devem ser Implementadas *Access Control List*s entre VLANs.	8	TEC	S	40,00	0,00	M	A	-
9	Deve haver *firewall* entre as VLANs.	8	TEC	N	80,00	15000,00	M	M	M
10	Deve haver IPS em todos os segmentos da LANs.	8	TEC	N	80,00	15000,00	M	M	M
11	NAC está implementado	8	TEC	N	80,00	15000,00	M	M	M
12	Utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory*.	8	TEC	N	80,00	10000,00	M	M	M
13	Deve ser utilizado protocolo de roteamento autenticado.	8	TEC	N	8,00	0,00	B	B	B

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
14	Deve haver sumarização de rotas.	8	TEC	N	40,00	0,00	B	B	B
15	Os *links* de dados através da WAN devem ser cifrados.	8	TEC	N	16,00	15000,00	B	B	B
16	Deve haver *switches* de reserva.	10	TEC	N	4,00	2000,00	B	B	B
17	Os *racks* de distribuição devem possuir ventilação adequada.	8	TEC	S	0,00	0,00	B	M	-
18	Os cabeamentos estruturados devem ser separados dos cabeamentos elétricos	8	TEC	S	0,00	0,00	B	B	-
19	A função *anti-snooping* deve ser habilitada nos *switches.*	8	TEC	S	4,00	0,00	B	A	-
20	O servidor DNS deve estar configurado conforme orientação do fabricante.	8	TEC	S	0,00	0,00	M	A	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
21	O parâmetro de atualização dinâmica de zona deve estar habilitado no servidor (Windows).	8	TEC	S	0,00	0,00	M	A	-
22	O DNS deve estar integrado ao *Active Directory*.	8	TEC	S	0,00	0,00	M	A	-
23	O IPSEC deve estar configurado na comunicação entre o ERP e o banco de dados.	8	TEC	N	16,00	0,00	B	M	B
24	Deve ser desativada a *community public* do SNMP.	8	TEC	N	8,00	0,00	B	B	B
25	A rede sem fio não deve propagar o SSID.	8	TEC	S	0,00	0,00	B	B	-
26	O filtro de endereços MAC deve estar habilitado na rede sem fio.	8	TEC	S	0,00	0,00	B	B	-
27	A criptografia da rede sem fio deve estar no modo WPA2.	8	TEC	S	0,00	0,00	B	M	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Todo dispositivo sem fio deve utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory*.	8	TEC	N	8,00	0,00	B	M	B
29	Os *firmwares* de todos os ativos de rede devem estar atualizados para a última versão.	8	TEC	N	40,00	0,00	B	M	B
30	O sinal da rede sem fio não deve propagar além do perímetro físico da empresa.	8	TEC	S	0,00	0,00	B	A	-
31	A conexão com dispositivos de rede sem fio deve ser desativada após 15 minutos sem uso.	8	TEC	N	8,00	0,00	B	B	B
32	Todos os ativos de rede devem ter as senhas padrão alteradas.	8	TEC	S	8,00	0,00	M	M	-

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
33	Garantir que o ponto de acesso está em local seguro.	4	TEC	S	0,00	0,00	B	B	-
34	Serviços acessíveis externamente devem estar na DMZ.	8	TEC	S	40,00	2000,00	A	A	-
35	O *Port Security* deve estar habilitado nos *switches.*	8	TEC	N	40,00	0,00	M	M	M
36	Deve haver um servidor de DHCP *backup* para distribuição de endereçamento IP.	8	TEC	N	6,00	0,00	B	B	B
37	Garantir que não existam *links* externos não gerenciados.	8	TEC	S	20,00	0,00	M	M	-

15.7.2 Resumo dos riscos

A Tabela 165 (Rede: riscos por intensidade) e a Figura 79 apresentam o resumo dos riscos aos quais a rede está sujeita.

Tabela 165: Rede: riscos por intensidade

Rede *esumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	6	33,33
B	**Baixo**	12	66,67

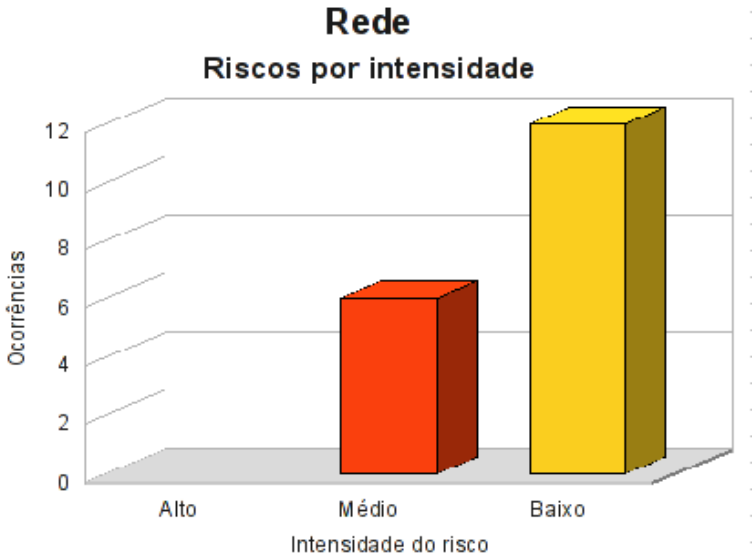


Figura 79: Rede: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 166 (Rede: riscos por tipo de vulnerabilidade) e a Figura 80.

Tabela 166: Rede: riscos por tipo de vulnerabilidade

Rede *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	0	0	6
B	**Baixo**	0	0	12

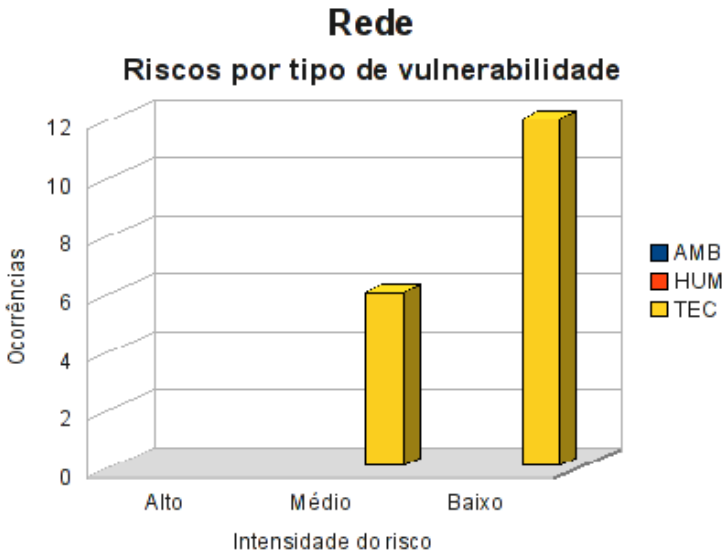


Figura 80: Rede: riscos por tipo de vulnerabilidade

15.7.3 Conformidade com os controles

A conformidade com os controles de segurança da rede é apresentada na Tabela 167 (Rede: conformidade com os controles) e o gráfico na Figura 81.

Tabela 167: Rede: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	18	48,65
Implementados	19	51,35
Total	**37**	**100,00**

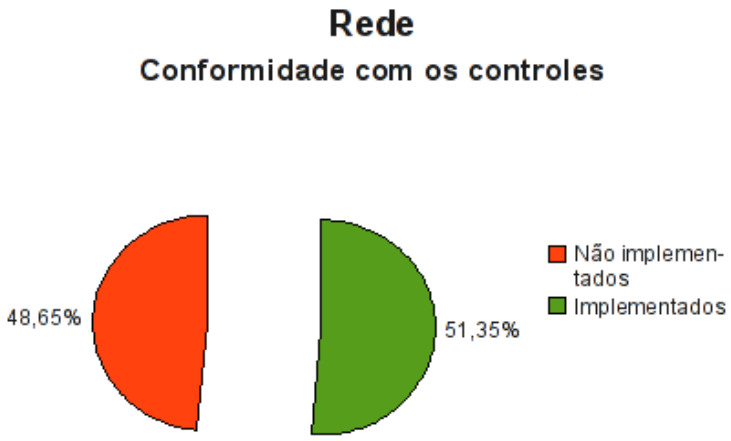


Figura 81: Rede: conformidade com os controles

15.7.4 Investimentos necessários

A Tabela 168 (Rede: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na rede.

Tabela 168: Rede: custo estimado para mitigar/controlar os riscos

Rede *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	534,00	37380,00
Investimento			84000,00
Total a ser investido			**121380,00**

A Tabela 169 (Rede*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na rede por intensidade dos riscos.

Tabela 169: Rede: custos por intensidade do risco

Rede *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	90760,00
B	**Baixo**	30620,00
Total		**121380,00**

15.8 Segurança física

A segurança física contava com 76,67% dos controles de segurança já implementados na primeira análise de risco.

15.8.1 Riscos e controles

O resultado da aplicação do *checklist* de controles é apresentado na Tabela 170 (Segurança física: controles).

Tabela 170: Segurança física: controles

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	O perímetro externo da empresa deve ter cerca com altura igual ou superior a 2,5 metros.	1	HUM	S	0,00	0,00	B	B	-
2	Deve haver sensores de invasão no perímetro da empresa.	1	HUM	N	40,00	10000,00	B	B	B
3	Deve haver guarda patrimonial 24 horas por dia.	1	HUM	S	0,00	0,00	A	A	-
4	O perímetro externo da empresa deve possuir placa de aviso de propriedade privada.	1	HUM	S	0,00	0,00	B	B	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Deve haver cães de guarda treinados.	1	HUM	S	0,00	0,00	M	M	-
6	Deve existir sistema de detecção e combate a incêndio.	1	AMB	S	0,00	0,00	B	A	-
7	As áreas criticas devem possuir controle de acesso.	1	TEC	S	8,00	4000,00	M	M	-
8	Devem ser elaborados registros de manutenção preventiva do sistema de alarme.	4	HUM	N	4,00	0,00	B	B	B
9	Deve haver câmeras de CFTV externas e internas e as imagens devem ser retidas por 180 dias.	1	HUM	S	40,00	18000,00	M	M	-
10	A brigada de incêndio deve ser treinada anualmente.	1	HUM	S	0,00	0,00	B	A	-
11	Todos os painéis de distribuição devem ser trancados.	1	HUM	S	0,00	0,00	B	M	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Os circuitos elétricos devem ser divididos e dimensionados adequadamente.	10	TEC	S	0,00	0,00	A	A	-
13	Devem ser instalados pára-raios para a proteção dos equipamentos e do prédio.	7	AMB	S	0,00	0,00	B	A	-
14	Deve haver uma malha de aterramento elétrico para os equipamentos elétricos e eletrônicos.	8	AMB	S	0,00	0,00	M	A	-
15	Todas as eletro-calhas e tubulações metálicas devem ser aterradas.	8	AMB	S	0,00	0,00	M	A	-
16	O grupo moto-gerador deve ser testado mensalmente.	8	TEC	N	4,00	0,00	B	M	B
17	Devem ser instaladas unidades de luz de emergência no interior da empresa.	8	TEC	S	0,00	0,00	B	B	-

Segurança física		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Todos os circuitos elétricos devem ser protegidos por disjuntores termomagnéticos.	8	TEC	S	0,00	0,00	A	A	-
19	Todos os circuitos elétricos devem ser identificados com etiquetas legíveis.	8	HUM	S	0,00	0,00	B	B	-
20	Deve ser elaborado um mecanismo de registro de incidentes de segurança física.	11	HUM	N	8,00	0,00	B	B	B
21	Todos os visitantes devem ser devidamente identificados, registrados e portar crachá em local visível.	4	AMB	S	0,00	0,00	B	A	-
22	O sistema de alarme de incêndio deve ser testado mensalmente e o teste deve ser registrado.	4	TEC	S	0,00	0,00	B	A	-

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Os extintores de incêndio devem ser inspecionados trimestralmente (com registro).	4	TEC	S	0,00	0,00	B	A	-
24	O cabeamento deve ser verificado quanto à conformidade com as normas de cabeamento estruturado.	10	TEC	S	0,00	0,00	A	M	-
25	Todos os cabos devem ser devidamente identificados.	10	TEC	S	0,00	0,00	B	B	-
26	Os cabeamentos de dados, telefonia e de energia elétrica devem ser instalados fisicamente separados.	8	TEC	S	0,00	0,00	A	M	-
27	Os cabos de dados do *data center* devem ser instalados diretamente (ponto-a-ponto) sem emendas.	8	TEC	S	0,00	0,00	A	M	-

Segurança física		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Os dutos de ar condicionado devem ser revestidos externamente por material térmico e não combustível.	4	TEC	S	0,00	0,00	A	A	-
29	Os equipamentos de refrigeração instalados externamente devem ser devidamente protegidos contra acesso físico não autorizado.	1	TEC	S	0,00	0,00	M	A	-
30	Os vidros da guarita de entrada devem ser escuros ou cobertos com película protetora escura.	1	AMB	S	0,00	200,00	M	M	-

15.8.2 Resumo dos riscos

A Tabela 171 (Segurança física: riscos por intensidade) e na Figura 82 apresentam o resumo dos riscos relacionados à segurança física.

Tabela 171: Segurança física: riscos por intensidade

Segurança física *Resumo dos riscos por intensidade*			
Nível		*Ocorrências*	*%*
A	**Alto**	0	0,00
M	**Médio**	0	0,00
B	**Baixo**	4	100,00

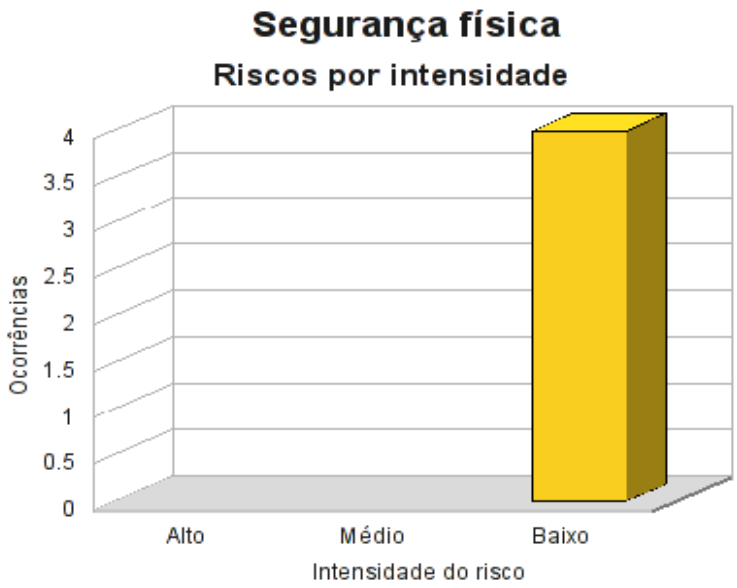


Figura 82: Segurança física: riscos por intensidade

Classificando os riscos pelo tipo de vulnerabilidade, obtemos o resultado apresentado na Tabela 172 (Segurança física: riscos por tipo de vulnerabilidade) e a Figura 83.

Tabela 172: Segurança física: riscos por tipo de vulnerabilidade

Segurança física *Resumo dos riscos por tipo de vulnerabilidade*				
Risco		*Ocorrências*		
		AMB	*HUM*	*TEC*
A	**Alto**	0	0	0
M	**Médio**	0	0	0
B	**Baixo**	0	3	1

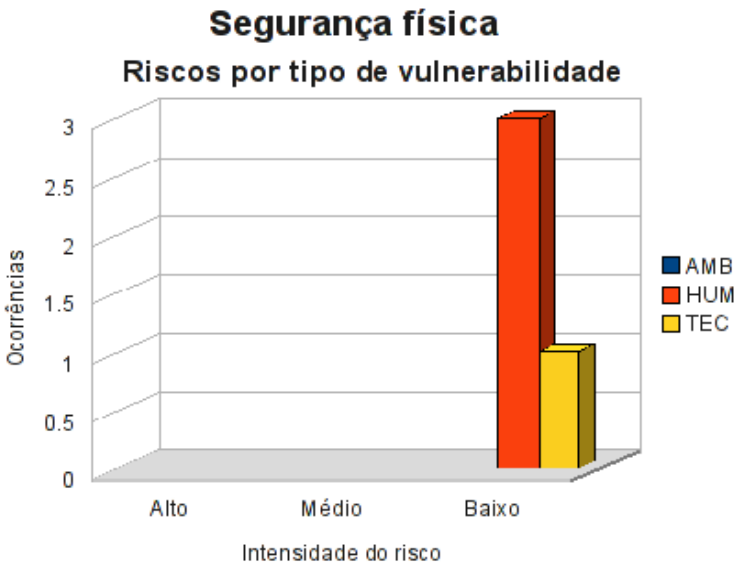


Figura 83: Segurança física: riscos por tipo de vulnerabilidade

15.8.3 Conformidade com os controles

A conformidade com os controles de segurança é apresentada na Tabela 173 (Segurança física: conformidade com os controles) e o gráfico, na Figura 84.

Tabela 173: Segurança física: conformidade com os controles

Conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	4	13,33
Implementados	26	86,67
Total	**30**	**100,00**

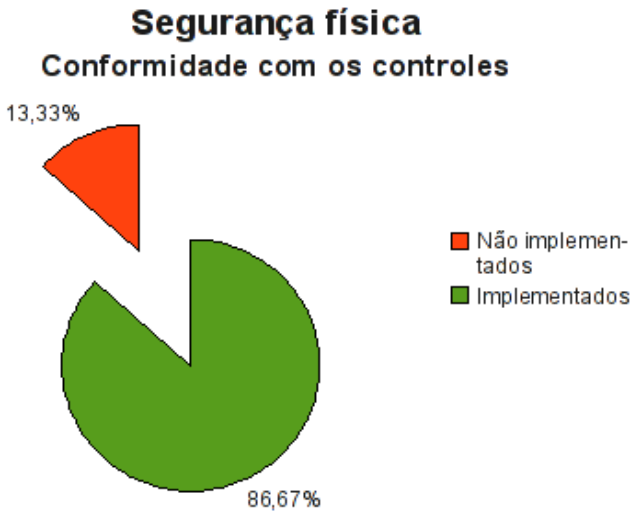


Figura 84: Segurança física: conformidade com os controles

15.8.4 Investimentos necessários

A Tabela 174 (Segurança física: custo estimado para mitigar/controlar os riscos) a seguir apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados.

Tabela 174: Segurança física: custo estimado para mitigar/controlar os riscos

Segurança física *Custo estimado para mitigar/controlar os riscos*			
	Valor HH (R$)	***Total HH (estimado)***	***Total (R$)***
Custo estimado	70,00	56,00	3920,00
Investimento			10000,00
Total a ser investido			**13920,00**

A Tabela 175 (Segurança física*:* custos por intensidade do risco) apresenta uma estimativa dos recursos financeiros necessários para o tratamento dos riscos encontrados na segurança física por intensidade dos riscos.

Tabela 175: Segurança física: custos por intensidade do risco

Segurança física *Custo estimado para mitigar/controlar os riscos* *(por intensidade do risco)*		
	Risco	***Custo + investimento (R$)***
A	**Alto**	0,00
M	**Médio**	0,00
B	**Baixo**	13920,00
Total		**13920,00**

15.9 Resumo executivo

Finalizada a segunda análise de risco os ativos da M2FE ainda não se encontram totalmente em conformidade com os controles de segurança, como pode ser observado na Tabela 176 (Resumo geral de conformidade com os controles) e representado no gráfico da Figura 85. Porém, pode ser observada uma sensível melhora na segurança dos ativos se comparado com o cenário encontrado na primeira análise de risco, onde havia apenas 21% dos controles implementados.

Tabela 176: Resumo geral de conformidade com os controles

Resumo geral de conformidade com os controles		
Controle	***Qde.***	***%***
Não implementados	45	11,54
Implementados	345	88,46
Total	**390**	**100,00**

Figura 85: Resumo geral de conformidade com os controles de segurança

Na Tabela 177 (Resumo dos custos e investimentos necessários) apresentamos o resumo dos custos e investimentos necessários para mitigar/controlar os riscos em cada um dos ativos analisados.

Tabela 177: Resumo dos custos e investimentos necessários

Custos e investimentos estimados necessários para mitigar/controlar os riscos				
Ativo	***Risco (R$)***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Firewall Netfilter	1.155,00	560,00	0,00	1.715,00
Firewall Netfilter - controles do sistema operacional Linux	0,00	0,00	0,00	0,00
Servidor de banco de dados	700,00	0,00	0,00	700,00
Servidor de banco de dados - controles do sistema operacional *Windows* 2003 *Server*	0,00	0,00	0,00	0,00
Servidor ERP	5.040,00	25.360,00	0,00	30.400,00
Servidor ERP - controles do sistema operacional *Windows* 2003 *Server*	0,00	0,00	0,00	0,00
Servidor *Windows Active Directory*	0,00	0,00	0,00	0,00
Servidor *Windows Active Directory* - controles do sistema operacional *Windows* 2003 *Server*	0,00	0,00	0,00	0,00
Servidor de arquivos	0,00	560,00	0,00	560,00
Servidor de Arquivos - controles do sistema operacional *Windows* 2003 *Server*	0,00	0,00	0,00	0,00
Data center	0,00	6.800,00	0,00	6.800,00

Custos e investimentos estimados necessários para mitigar/controlar os riscos				
Ativo	***Risco (R$)***			***Total (R$)***
	Baixo	***Médio***	***Alto***	
Rede	30.620,00	90.760,00	0,00	121.380,00
Segurança física	13.920,00	0,00	0,00	13.920,00
Total (R$)	**51.435,00**	**124.040,00**	**0,00**	**175.475,00**

Como a segurança é um processo contínuo, mesmo tendo conseguido alcançar uma melhora na segurança de seus ativos, a M2FE deve continuar o plano de segurança e implementar todos os controles de segurança, começando preferencialmente pelos controles referentes aos riscos de alta intensidade, passando pelos de média e, finalmente, os de baixa intensidade.

16 EVOLUÇÃO DA CONFORMIDADE AOS ITENS DE CONTROLE

Sempre que um objeto é avaliado várias vezes no decorrer do tempo, é natural que se deseje comparar os resultados destas avaliações de forma a obtermos alguma visualização da evolução do objeto. Com relação às análises de risco, podemos compará-las de várias formas. Como o ambiente da M2FE manteve-se estável no período das análises, isto é, não houve alterações de processos e nem de ativos, uma forma de comparar os resultados das análises consiste em verificar a conformidade dos ativos aos itens de controle avaliados. Esta comparação nos permite verificar os efeitos dos trabalhos executados.

Na Tabela 178 (Evolução de conformidade) é apresentada a evolução da conformidade aos os itens de controle de segurança de cada ativo usando como base as informações obtidas nas duas análises de risco executadas.

Tabela 178: Evolução de conformidade

Controles implementados (%)		
Ativo	***Primeira análise***	***Segunda análise***
Firewall	13,11	85,25
Banco de dados	12,31	95,38
Servidor ERP	10,94	89,06
Servidor AD	11,86	100,00
Servidor de arquivos	10,17	98,31

Controles implementados (%)		
Ativo	***Primeira análise***	***Segunda análise***
Data center	66,67	80,00
Rede	35,14	51,35
Segurança física	76,67	86,67

Pode-se constatar que houve uma melhora significativa na segurança dos ativos, pois todos eles tiveram um aumento no número de controles de segurança implementados, como pode ser observado, graficamente, na Figura 86, na Figura 87 e na Figura 88.

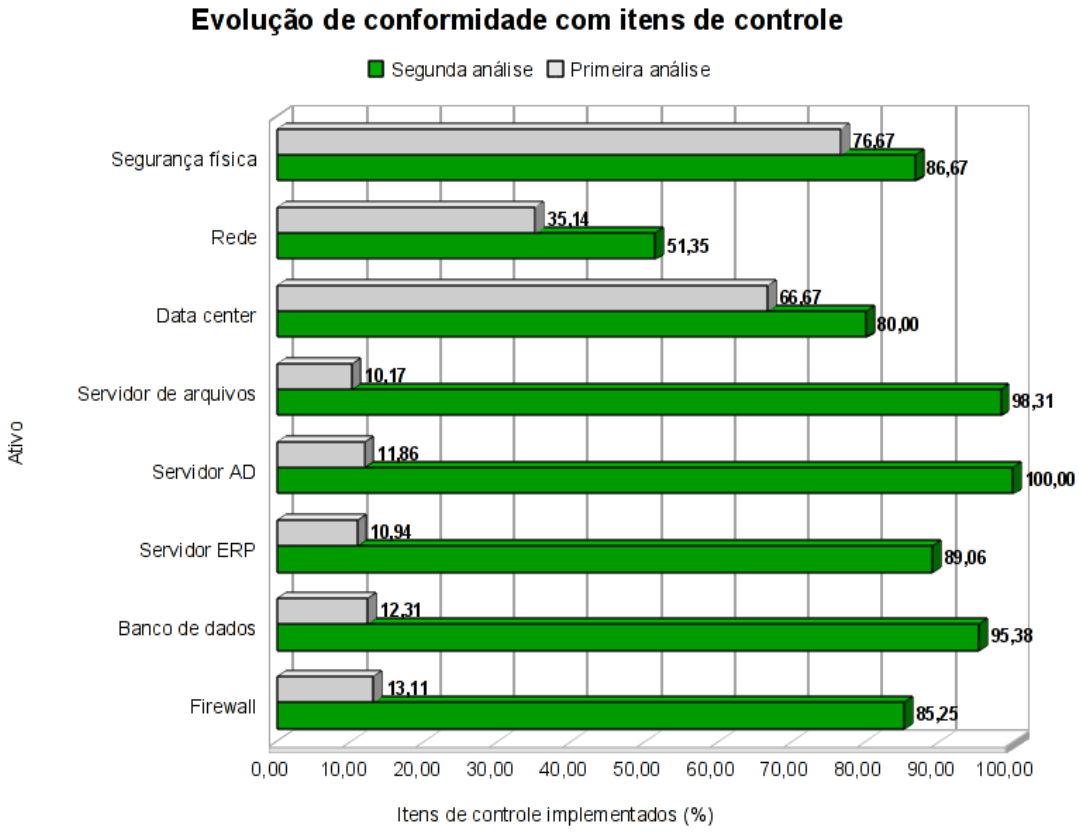


Figura 86: Evolução de conformidade

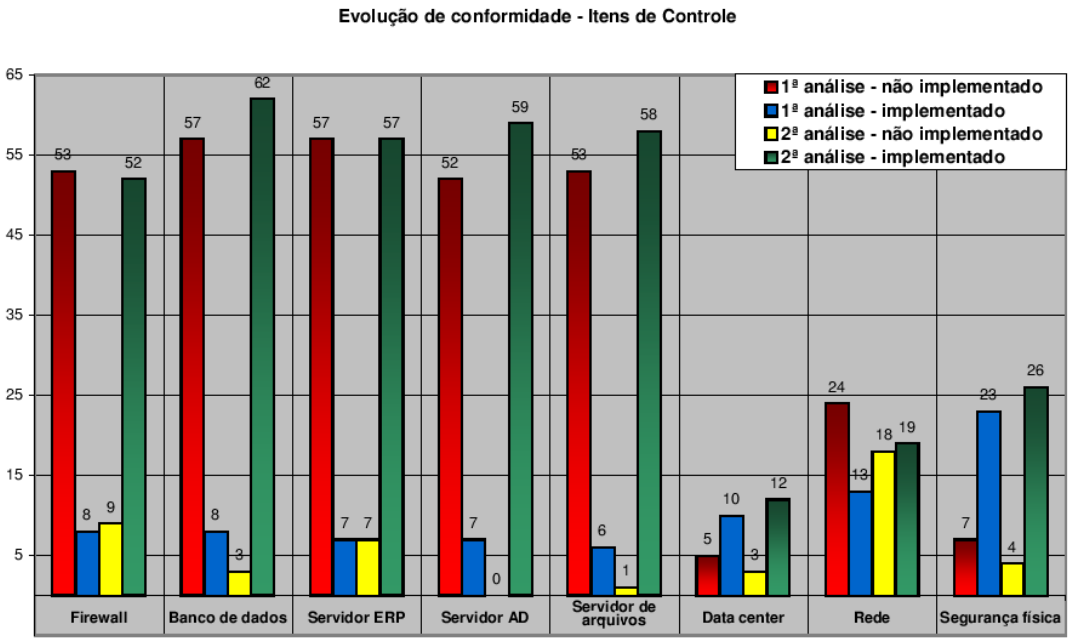


Figura 87: Evolução de conformidade: itens de controle

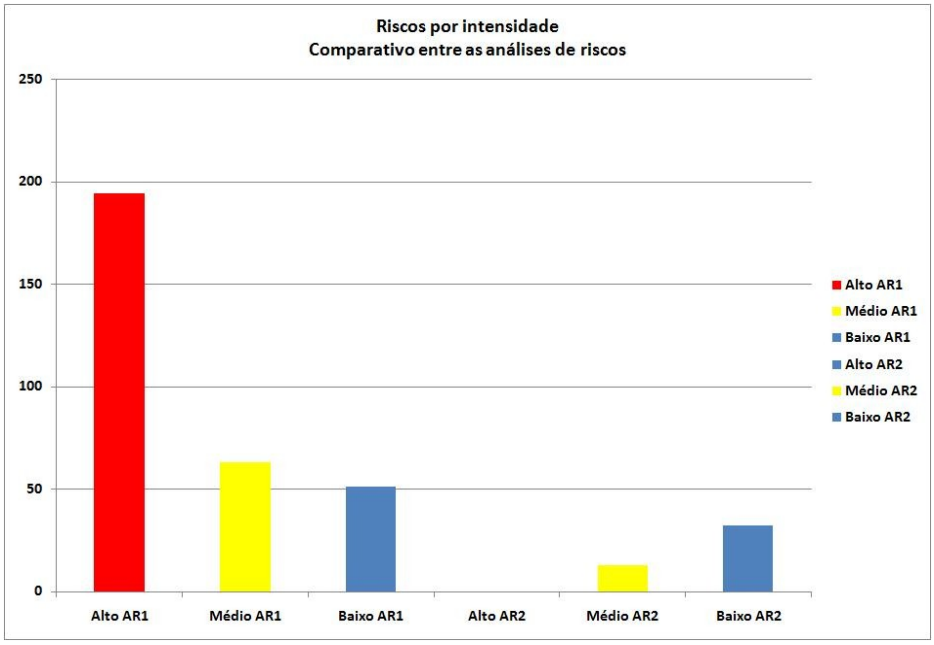


Figura 88: Comparativo entre as análises

Comparando-se os resultados das duas análises de riscos, observa-se que foi realizado um trabalho muito grande para minimizá-los mas, mesmo assim, nem todos os riscos foram mitigados, eliminados, aceitos ou transferidos. Ainda há controles a serem implementados e, portanto, a busca pela segurança da informação deve ser contínua.

17 GESTÃO DA SEGURANÇA DA INFORMAÇÃO

O processo de gestão da segurança da informação da M2FE utiliza como base a norma ABNT NBR ISO/IEC 27001:2006 (NBR ISO/IEC 27001, 2006).

17.1 Objetivo

A gestão da segurança da informação na M2FE foi desenvolvida de forma a garantir que os controles de segurança utilizados estejam adequados ao negócio da empresa e que garantam a proteção dos ativos de informação, de maneira contínua.

17.2 Abordagem do processo

A gestão de segurança da informação da M2FE determina que os colaboradores, de acordo com as suas responsabilidades:

- Compreendam todos os requisitos de segurança da organização e a importância das políticas e objetivos.
- Garantam que os requisitos de segurança definidos sejam implementados e seguidos a fim de mitigar, controlar ou aceitar os riscos da segurança da informação.
- Monitorem e analisem criticamente a eficiência do SGSI.
- Proporcionem a melhoria contínua do SGSI.

A M2FE adota o modelo conhecido como "*Plan – Do – Check – Act"* (PDCA) conforme Figura 89.

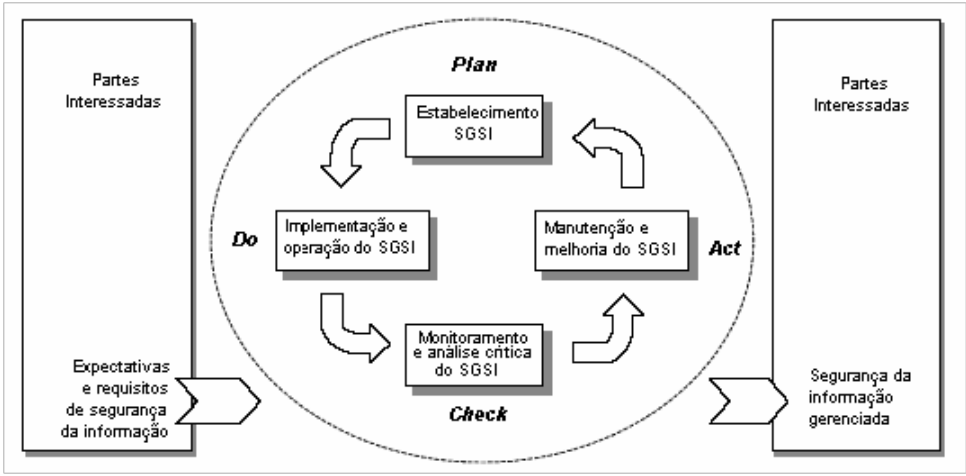


Figura 89: Modelo PDCA, extraído de (NBR ISO/IEC 27001, 2006)

Tabela 179: Modelo PDCA, conforme (NBR ISO/IEC 27001, 2006)

Plan (planejar) (planejar o SGSI)	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) (implementar e operar o SGSI)	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (verificar) (monitorar e analisar criticamente o SGSI)	Avaliar e, quando aplicável, medir o desempenho de um processo frente à política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção.
Act (agir) (manter e melhorar o SGSI)	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.

17.3 Estabelecendo e gerenciando o SGSI

O SGSI na M2FE seguiu as etapas apresentadas a seguir.

17.3.1 Estabelecer

A primeira fase do ciclo PDCA é o planejamento (*Plan*), no qual deve-se definir o escopo e a abrangência do SGSI, alinhado aos requisitos de negócio da M2FE e da legislação; definir os riscos envolvidos e seus critérios de avaliação; identificar, analisar e avaliar os riscos e as opções de tratamento e controles; obter aprovação da direção relacionada aos riscos residuais e obter a autorização para a implementação.

As seguintes ações devem ser estabelecidas na M2FE:

- Deve existir um CSO respondendo diretamente à presidência.
- Elaborar e manter a metodologia de análise de riscos.
- Criar o comitê de segurança.
- Definir diretrizes, políticas técnicas, políticas de uso, procedimentos, classificação da informação e padrões de *software* e *hardware*.
- Elaborar e manter o PCN.

17.3.2 Implementar e operar

Nesta fase é implementado o plano de tratamento de riscos, as ações de gestão necessárias, os recursos, as responsabilidades, os treinamentos necessários e os programas de conscientização.

As seguintes ações devem ser implementadas na M2FE:

- Executar a análise de riscos anualmente ou quando um processo, sistema ou ativo for criado ou alterado.
- Treinar os colaboradores em segurança da informação.

- Diretrizes e políticas de segurança.
- Controles resultantes da análise de riscos.

17.3.3 Monitorar e analisar criticamente

Acompanhar e controlar o que está sendo realizado, de modo a propor ações corretivas e preventivas no menor espaço de tempo possível após a detecção da anormalidade.

As seguintes ações devem ser monitoradas e analisadas na M2FE:

- Monitorar os controles especificados na análise de risco conforme metodologia.
- Executar auditorias internas anualmente ou quando necessário.
- Acompanhar mensalmente os chamados de *Help Desk* para verificação de incidentes de segurança.
- Analisar mensalmente os relatórios de incidentes reportados pelo comitê de segurança.

17.3.4 Manter e melhorar

As melhorias identificadas nos passos anteriores devem ser implementadas no SGSI, comunicando a todos os interessados as alterações ocorridas, usando como base as lições aprendidas e assegurando que as melhorias atinjam os objetivos pretendidos.

As seguintes ações devem ser mantidas na M2FE:

- Atualizar as diretrizes e políticas de segurança conforme a validade das mesmas ou quando definido pelo Comitê de Segurança.
- Atualizar os *checklists* e procedimentos técnicos anualmente ou quando necessário.
- Atualizar a metodologia de análise de riscos anualmente ou quando necessário.
- Atualizar anualmente o programa de treinamento e conscientização de segurança da informação.

- Comunicar todas as alterações aos interessados.
- Treinar e conscientizar continuamente todos os colaboradores.

17.4 Requisitos de documentação

A documentação registra as decisões do corpo técnico e diretivo; a rastreabilidade das ações; as diretrizes, políticas, procedimentos e controles adotados pela empresa e a metodologia de análise e avaliação de riscos, bem como todos os seus relatórios. Toda documentação deve ser aprovada, protegida, controlada e divulgada aos interessados.

Os seguintes documentos devem ser utilizados na M2FE:

- Carta do presidente.
- Termo de responsabilidade, compromisso e sigilo.
- Diretrizes, políticas técnicas, políticas de uso, procedimentos e padrões.
- Plano de Continuidade de Negócio.
- Metodologia de análise de riscos.
- *Checklists* de controles para análise de riscos.
- Gestão de segurança da informação.

17.5 Responsabilidade da direção

A direção da empresa está comprometida com o SGSI garantindo os planos e objetivos, definindo papéis e responsabilidades, comunicando à organização a importância em atender os objetivos da segurança da informação, a conformidade com a política de segurança e provendo apoio aos gestores.

As seguintes ações são responsabilidade da direção da M2FE:

- Contratar o CSO respondendo diretamente à presidência.

- Criar e manter o comitê de segurança.
- Prover aportes necessários para a implementação dos controles identificados na análise de riscos.
- Divulgar a carta do presidente.
- Prover recursos para aquisição de materiais e acessórios para a realização dos treinamentos em segurança da informação.

17.6 Auditorias

A organização conduz auditorias internas do SGSI anualmente a fim de verificar se os objetivos de controle, processos e procedimentos atendem às necessidades da organização e legislação.

A seguinte ação deve ser executada na M2FE:

- Avaliar anualmente ou quando necessário os procedimentos executados pelo SGSI para verificação quanto à aderência ao negócio.

18 BENEFÍCIOS ALCANÇADOS COM O PLANO DE SEGURANÇA DA INFORMAÇÃO

Após a contratação do CSO e com as medidas implementadas, a M2FE conseguiu alcançar os seguintes benefícios:

- Comprometimento da direção com a gestão da segurança da informação.
- Criação das políticas de segurança
- Classificação das informações, melhorando a sua gerência.
- Implementação de rotinas de *backup*.
- Treinamentos e conscientização dos colaboradores em segurança da informação .
- Criação do Plano de Continuidade de Negócios.
- Definição e implementação da análise de riscos.
- Criação e gerenciamento de mecanismos de controle de acesso físico e lógico.
- Segmentação da rede.
- Segregação de função nos sistemas
- Gestão da segurança da informação

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 17799:2005*: Tecnologia da informação - técnicas de segurança - código de prática para a gestão da segurança da informação. Rio de Janeiro, jul. 2005.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001:2006*: Tecnologia da informação - técnicas de segurança - sistemas de gestão de segurança da informação - requisitos. Rio de Janeiro, 2006.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27005:2008*: Tecnologia da informação - técnicas de segurança - gestão de riscos de segurança da informação. Rio de Janeiro, 2008.

BARMAN, S. *Writing Information Security Policies*. USA: New Riders, 2001.

DOMINGOS, C.; MARUYAMA, T.; MELO, S. *BS7799 - Da Tática à Prática em Servidores Linux*. Brasil: Alta Books, 2006.

DERY, A. *Hardening Debian 4.0 - Creating a simple and solid foundation for your applications*. EUA: SANS Institute Reading Room Site, 2009. Disponível em 16/Julho/2009 em http://www.sans.org/reading_room/whitepapers/linux/hardening_debian_4 _0_-creating_a_simple_and_solid_foundation_for_your_applications_2059.

CISECURITY. THE CENTER FOR INTERNET SECURITY. *Center for Internet Security Ben-chmark for Debian Linux v1.0*. EUA, 2007. Disponível em 26/Julho/2009 em https://community.cisecurity.org/download/?redir=/linux/CIS_Debian_Benchmark_v1.0.pdf.

DISA. DEFENSE INFORMATION SYSTEMS AGENCY. *Windows Server 2003 Security Checklist: Checklist*. EUA, Junho 2009. Disponível em 26/Julho/2009 em http://iase.disa.mil/stigs/checklist/windows_2003_checklist_v6r1-12_2009_06_26.zip.

DISA. DEFENSE INFORMATION SYSTEMS AGENCY. *Enterprise Resource Planning Checklist: For generic implementations*. EUA, Abril 2007. Disponível em 26/Julho/2009 em http://iase.disa.mil/stigs/checklist/erp-generic-checklist-v1r1-1-20070410.doc.

DISA. DEFENSE INFORMATION SYSTEMS AGENCY. *Oracle Database Security Checklist: Version 8, release 1.3*. EUA, Março 2009. Disponível em 26/Julho/2009 em http://iase.disa.mil/stigs/checklist/db_srr_checklist_oracle_v8r1-3.pdf.

HARRIS, S. *All in one CISSP Exam Guide - Fourth Edition*. USA: McGraw Hill, 2007.

STONEBURNER, G.; GOGUEN, A.; FERINGA, A. *SP-800-30 - Risk Management Guide for Information Technology Systems.* USA: NIST National Institute os Standards and Technology, 2002.

WALLACE, K.; WATKINS, M. *CCNA Security - Official Exam Certification Guide*. Indianapolis, USA: Cisco Press, 2008.

SUEHRING, S.; ZIEGLER, R. L. *Linux Firewalls, Third Edition*. Indianapolis, Indiana, USA: Novell Press, 2005.

ACRÔNIMOS

ABNT	Associação Brasileira de Normas Técnicas.
ACL	*Access Control List.*
AD	*Active Directory.*
ADSL	*Asymmetric Digital Subscriber Line.*
ARP	*Address Resolution Protocol.*
BIA	*Business Impact Analysis.*
BSI	*British Standard Institute.*
CFTV	Circuito Fechado de Televisão.
COBIT	*Control Objectives for Information and related Technology.*
CSO	*Chief Security Officer.*
DAT	*Digital Audio Tape.*
DBA	*Database Administrator.*
DDL	*Data Definition Language.*
DHCP	*Dynamic Host Configuration Protocol*.
DMZ	*Demilitarized Zone.*

DNS *Domain Name System.*

DSL *Digital Subscriber Line*.

DVR *Digital Video Recorder.*

ERP *Enterprise Resource Planning.*

FSMO *Flexible Single-Master Operation.*

FTP *File Transfer Protocol.*

GB Gigabyte

GNU *GNU's Not Unix.*

GPO *Group Police.*

GRUB *GRand Unified Bootloader.*

IAS *Internet Authentication Service.*

ICMP *Internet Control Message Protocol.*

IEC *International Electrotechnical Commission.*

IIS *Internet Information Services.*

IP *Internet Protocol.*

IPS *Intrusion Prevention System.*

IPSEC *Internet Protocol Security.*

ISO *International Organization for Standardization.*

LAN *Local Area Network.*

MAC *Media Access Control.*

MHz Megahertz.

MPLS *Multiprotocol Label Switching.*

NAC *Network Admission Control.*

NBR Norma Brasileira

NFS *Network File System.*

Nodev *No device.*

Noexec *No execute.*

Nosuid *No Set User ID.*

NTFS *New Technology File System.*

NTP *Network Time Protocol.*

PAC Plano de Administração de Crise.

PAM *Pluggable Authentication Modules.*

PCN Plano de Continuidade dos Negócios.

PCO Plano de Continuidade Operacional.

PCP Planejamento e Controle da Produção.

PDCA *Plan, Do, Check, Act.*

PRD Plano de Recuperação de Desastres.

QoS *Quality of Service.*

RAM *Random Access Memory.*

RFC *Request For Comments.*

RTO *Recovery Time Objective.*

SAM *Security Accounts Manager.*

SGID	*Set Group ID.*
SGSI	Sistema de Gestão da Segurança da Informação.
SI	Segurança da Informação.
SLA	*Service Level Agreement.*
SSH	*Secure Shell.*
SSID	*Service Set Identifier.*
STP	*Spanning Tree Protocol.*
SUID	*Set User ID.*
TCP/IP	*Transmission Control Protocol / Internet Protocol.*
TI	Tecnologia da Informação.
URL	*Uniform Resource Locator*.
USB	*Universal Serial Bus.*
VLAN	*Virtual Local Area Network.*
VoIP	*Voice over Internet Protocol.*
VPN	*Virtual Private Network* .
WEB	WWW (*World Wide Web*).
WPA	*Wi-Fi Protected Access.*

GLOSSÁRIO

.NET *passports*	Autenticação única que usa o endereço de *e-mail* para fornecer acesso personalizado a serviços e sites habilitados para o *Passport.*
Access Control List	Lista de controle de acesso.
Active Directory	Implementação de serviço de diretório no protocolo LDAP que armazena informações sobre a rede de computadores e as disponibiliza a usuários e administradores da rede
Active Directory Schema Master	Controla todas as atualizações no *Schema* que contém a lista *master* de classes de objetos e atributos que são usados para a criação de objetos como usuários, impressoras etc.
ActiveX	É um conjunto de tecnologias (software) criado pela Microsoft para facilitar a integração entre diversas aplicações.
Address Resolution Protocol	Protocolo de resolução de endereço. É um protocolo usado para encontrar um endereço da camada de enlace de rede.
Agendador de tarefas	É um *software* que permite agendar a execução de tarefas (*softwares*) em data e horários pré-estabelecidos.

Agente de ameaça	Intenção e método que visa explorar intencionalmente uma vulnerabilidade; ou situação e método que pode acidentalmente disparar uma vulnerabilidade.
Ameaça	Potencial de um agente da ameaça explorar uma vulnerabilidade específica, acidental ou intencionalmente.
Anti-snooping	Técnica que impede a leitura e decodificação da informação em trânsito.
Apache	Servidor HTTP web livre.
Assinatura digital	É processo de associar uma mensagem a uma entidade provendo autenticação, integridade e não-repúdio. A assinatura digital prova a origem da mensagem.
Asymmetric Digital Subscriber Line	É um formato de DSL, uma tecnologia de comunicação de dados que permite uma transmissão de dados mais rápida através de linhas de telefone do que por modem.
Ativo	É qualquer bem que possua algum valor para a empresa.
Backup	Cópia dos dados em outro local de forma que os mesmos possam ser recuperados em caso de desastre.
Banner	Mensagem apresentada por *softwares* durante o acesso de um cliente ou em determinadas situações.
Broadcast	Uma mensagem enviada para todos os dispositivos que estão no mesmo segmento de rede.
BS 25999	Norma Britânica para Gestão da Continuidade do Negócio.

Business Impact Analysis	Processo de análise utilizado para revelar os impactos empresariais resultantes da paralisação de um processo crítico por um período que exceda o tempo máximo permissível.
Cavalo de tróia	Programa, normalmente recebido sob o pretexto de outro objetivo (por exemplo um cartão virtual), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.
Chat	Aplicação de conversação em tempo real.
Checklist	Lista contendo itens a serem verificados.
Chief Security Officer	Profissional responsável pela segurança da empresa, sendo responsável pelo desenvolvimento, implementação e gerenciamento das estratégias e programas de segurança da corporação.
CISCO IOS	Sistema operacional da CISCO.
COBIT	É um guia de boas práticas apresentado como *framework*, dirigido para a gestão de tecnologia de informação.
Colaboradores	Funcionários, estagiários e prestadores de serviços.
Cold-Site	Alternativa de contingência a partir de um ambiente com os recursos mínimos de infraestrutura e telecomunicações.
Community public	Uma *string* utilizada pelo agente SNMP para identificar que tipo de dados um agente SNMP vai ter acesso.
Conexão anônima	Conexão que não exige autenticação.
Confidencialidade	Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.

Controle de acesso	Mecanismo que permite ou nega o acesso a um recurso.
Core dump	A ação de determinados sinais enviados pelo sistema operacional ou pelo usuário a um programa em execução causam a finalização do programa produzindo um *core dump*, que é uma arquivo contendo a imagem da memória do processo no instante da sua finalização.
Cracker	Indivíduo que quebra um sistema de segurança, de forma ilegal e sem ética.
Data center	Local onde são concentrados os computadores, sistemas e *softwares* responsáveis pelo processamento de dados de uma empresa ou organização.
Data Definition Language	Linguagem utilizada para a definição de estruturas de dados em bancos de dados.
Database Administrator	Administrador de banco de dados.
Debian	É simultaneamente o nome de uma distribuição não comercial livre (gratuita e de código fonte aberto) de *GNU/Linux* (amplamente utilizada) e de um grupo de voluntários que a mantêm.
Demilitarized Zone	Zona Desmilitarizada (DMZ). A DMZ é uma rede situada entre uma rede confiável e uma rede não confiável. A aplicação típica da DMZ é colocá-la entre uma rede local e a *Internet.* Sua função é manter todos os serviços que possuem acesso externo separados da rede local.
Digital Subscriber Line	Família de tecnologias que fornecem um meio de transmissão digital de dados, aproveitando a própria rede de telefonia.
Digital Video Recorder	Sistema de gravação de vídeo.

Disaster Recovery Institute International	Instituto de capacitação e formação de profissionais em continuidade de negócios e recuperação de desastres com base em Washington.
Disponibilidade	Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação, no momento em que for requisitada.
Domain Name System	Sistema de gerenciamento de nomes hierárquico e distribuído utilizado para traduzir nomes de *hosts* em seus respectivos endereços de rede (IP).
Download	É a transferência de dados de um computador remoto para um computador local.
Driver	Programa utilizado para realizar a interface entre o *hardware* e o sistema operacional.
Dynamic Host Configuration Protocol	Protocolo de serviço TCP/IP que oferece configuração dinâmica de terminais, com concessão de endereços IP de host e outros parâmetros de configuração para clientes de rede
e-learning	Ensino a distância que possibilita a auto-aprendizagem, com a mediação de recursos didáticos sistematicamente organizados, apresentados em diferentes suportes tecnológicos de informação, utilizados isoladamente ou combinados, e veiculado através da internet.
E-mail	Correio eletrônico.
Enterprise Resource Planning	Sistemas de informações que integram dados e processos de uma organização em um único sistema.

Firewall	Dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto de controle da rede.
Firmware	É o conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico.
Flag	É um mecanismo lógico que funciona como um sinalizador e é utilizado normalmente em sistemas para indicar se um recurso do está ou não habilitado.
Flexible Single-Master Operation	Regras configuradas no *AD* (*Active Directory*) usadas para prevenir conflitos na replicação dos dados do *AD.*
Freeware	É qualquer programa de computador cuja utilização não implica o pagamento de licenças de uso ou *royalties*.
Full mesh	Arquitetura de rede na qual cada ponto é capaz de encontrar qualquer outro ponto diretamente através de uma conexão ponto-a-ponto física ou de um circuito lógico.
Gateway	Um dispositivo intermediário que se destinada a interligar redes, separar domínios de colisão ou mesmo traduzir protocolos.
Global catalog	Repositório de dados distribuído que contém parte de cada objeto de cada domínio de uma floresta do *Active Directory.*
GNU's Not Unix	Projeto lançado em 1984 para desenvolver um sistema operacional completo compatível com Unix e de livre utilização.
GNU/Linux	Sistema operacional que segue o padrão Unix constituído pelo *kernel* (núcleo) Linux adicionado das ferramentas GNU. Este sistema operacional é desenvolvido por centenas de programadores ao redor do mundo.

Grand Unified Bootloader	Multi-carregador de sistema operacional que, ao ser instalado no computador, permite que o usuário selecione o sistema operacional instalado no computador a ser iniciado.
Group Police	Recurso de configuração utilizado em sistemas Windows que permite a atribuição de regras de configurações de maneira automática.
Grupo wheel	Grupo de usuários do Linux. Normalmente os usuários participantes do grupo *wheel* possuem algum acesso administrativo.
guest	Conta de usuário visitante.
Hardcoded	São parâmetros fixos escritos diretamente no código da aplicação sem a possibilidade de alteração na inicialização do programa.
Hardening	Processo de mapeamento das ameaças, mitigação dos riscos e execução das atividades corretivas em um ativo de rede.
Hash	Função computacionalmente eficiente que mapeia cadeias binárias de tamanho arbitrário para cadeias binárias de tamanho fixo qualquer.
Home banking	Nome dado ao acesso aos serviços bancários efetuados remotamente, pela *Internet.*
Host	Máquina ou computador conectado a uma rede.
IEEE 802.1x	Mecanismo de autenticação para dispositivos em rede.
Integridade	A exatidão ou completeza do estado da informação no momento de sua geração e resgate.

Internet	Conglomerado de redes que interligam computadores em uma mesma rede, permitindo o acesso a informações e todo tipo de transferência de dados.
Internet Authentication Service	Implementação da Microsoft do serviço RADIUS para *Windows Server* 2003. Este serviço implementa a autenticação de conexão centralizada para vários tipos de acesso, incluindo redes sem fio e conexões VPN. O IAS também pode operar como um *proxy* para o serviço RADIUS, repassando as mensagens de autenticação para outros servidores.
Internet Control Message Protocol	Protocolo integrante da suíte de protocolos TCP/IP utilizado para envio de mensagens de controle da rede, tais como controle de fluxo, detecção de destinos não encontrados, redirecionamento de rotas e verificação da existência de *hosts* na rede.
Internet Information Services	Servidor *web* criado pela Microsoft.
Internet Protocol	Protocolo definido pela RFC791 que tem por objetivo interconectar redes de computadores fim-a-fim. Representa a camada três do modelo OSI e é um protocolo endereçado e roteável. É o protocolo utilizado na *Internet*.
Intranet	O conceito é o mesmo da *Internet*, mas o acesso não é aberto, ou seja, apenas pessoas autorizadas podem acessar uma *intranet*. Normalmente, é usada por empresas ou instituições para comunicação entre os seus colaboradores.
IP Forward	Nome dado ao processo de transferência de pacotes de uma interface para outra num *host* com múltiplas interfaces de rede.

IPSec	Protocolo de segurança IP é uma extensão do protocolo IP.
Netfilter	Filtro de pacotes implementado no *kernel* do *GNU/Linux*. O programa executado no espaço do usuário utilizado para administrar as regras de filtragem de pacotes do sistema operacional *GNU/Linux* é chamado *IPTables*. Muitas vezes, o termo *IPTables* é utilizado como sinônimo de filtro de pacotes do *GNU/Linux*, porém, a rigor, o filtro de pacotes propriamente dito é implementado no *kernel* e é o *Netfilter*, enquanto que *IPTables* é a ferramenta utilizada para administrar as regras do filtro de pacotes do *kernel* (*Netfilter*).
ISO/IEC 17799:2005	Norma Brasileira, Tecnologia da Informação — Técnicas de Segurança — Código de Prática para a gestão da segurança da informação.
LAN Manager	Sistema operacional de rede, desenvolvido pela Microsoft.
Lenny	Codinome da versão 5.0 do sistema operacional *Debian GNU/Linux*.
Listener	Processo executado em um *host* que atende conexões recebidas e as repassa para um processo específico. No caso específico do sistema gerenciador de banco de dados Oracle, *listener* é o nome de um componente do sistema que aguarda conexões numa determinada porta (1521 por padrão) e repassa as conexões para o componente de baco de dados.
Log	Registro de eventos em um sistema de computadores.
Media Access Control Address	Numa rede local, o endereço MAC define o endereço físico do dispositivo conectado à rede. Numa rede *Ethernet*, corresponde ao endereço *Ethernet*.

Mídias removíveis	Unidades de armazenamento facilmente destacáveis do computador, tais como fitas, *flash disks*, discos removíveis, CDs e DVDs.
Multiprotocol Label Switching	O MPLS (*Multiprotocol Label Switching*) é um protocolo de roteamento baseado em pacotes rotulados, no qual rótulo representa um índice na tabela de roteamento do próximo roteador. Pacotes com o mesmo rótulo e mesma classe de serviço são distinguíveis entre si e por isso recebem o mesmo tipo de tratamento.
Myspace	Serviço de rede social que utiliza a *Internet* para comunicação *online* através de uma rede interativa de fotos, *blogs* e perfis de usuário.
NBR ISO/IEC 27001:2006	Norma Brasileira para Sistemas de Gestão de Segurança da Informação - Requisitos.
Network Admission Control	Controle de acesso à rede local.
Network File System	Sistema de arquivos utilizado para compartilhar arquivos entre computadores conectados através de uma rede.
Network Time Protocol	Protocolo para sincronização de hora.
New Technology File System	Sistema de arquivos padrão para sistemas operacionais *Microsoft*.
Notebook	Computador portátil.
NTLMv2	Sistema de autenticação para acesso a compartilhamentos de arquivos.
Orkut	Uma rede social filiada ao *Google.*

Pluggable Authentication Modules	Em ambientes *Unix* e *Linux*, são módulos plugáveis ao sistema que permitem a adição de novos mecanismos de autenticação.
Plugin	Programa de computador que serve normalmente para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica.
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.
Ponto de acesso	Dispositivo que atua como como ponte entre uma rede sem fio e uma rede tradicional.
Portmap	Serviço gerenciador de RPC (*Remote Procedure Call*) usado para mapear um número de serviço RPC específico que um cliente está solicitando acesso e a porta do serviço na qual o serviço está efetivamente operando.
Proxy	Servidor que atende a requisições repassando os dados a outros servidores.
Quality of Service	Qualidade do serviço.
Rack	Estrutura geralmente metálica que hospeda os ativos de rede.
Random Access Memory	Memória de acesso aleatório. É neste tipo de memória que os programas de computador são carregados e executados.
Recovery Time Objective	Quando o assunto é continuidade do negócio, *Recovery Time Objective* é o tempo máximo no qual um processo de negócio deve ser restaurado após a ocorrência de um desastre de forma a evitar consequências inaceitáveis associadas à quebra da continuidade do negócio.

Red Hat Advanced Server	Sistema operacional *GNU/Linux* desenvolvido pela empresa *Red Hat*.
Red Hat Enterprise Linux	Sistema operacional *GNU/Linux* desenvolvido pela empresa *Red Hat*.
Request For Comments	Documentos publicado através do *Internet Society* ou da *Internet Engineering Task Force* (IETF), sendo que alguns deles acabam por tornar-se padrões. Tipicamente, as RFCs tratam de assuntos relacionados à *Internet* ou à pilha de protocolos TCP/IP.
RFC1918	RFC sobre a atribuição de endereços privados para a *Internet.*
Risco	É a probabilidade de um evento ocorrer e as suas consequências.
Roteador	Equipamento usado para fazer a comutação de protocolos, a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si.
Schema Master	Parte central do *Active Directory*, composto de objetos e atributos que modelam o *Active Directory*.
Secure Shell	É simultaneamente, um programa de computador e um protocolo de rede que permite a conexão com outro computador na rede usando um canal cifrado.
Security Accounts Manager	Banco de dados de usuários dos sistemas operacionais *Windows*.
Security Officer	Principal responsável por questões relacionadas com a segurança de uma organização.

Senha Frase, palavra-chave ou conjunto de caracteres utilizado para identificar o usuário ou sistema perante outro sistema, de forma a garantir-lhe ou não o acesso.

Service Level Agreement É um documento formal, negociado entre as partes, na contratação de um serviço de TI ou telecomunicações que tem por objetivo especificar os requisitos mínimos aceitáveis para o serviço proposto. O não cumprimento do SLA implica penalidades, estipuladas no contrato, para o provedor do serviço.

Service Set Identifier Conjunto de caracteres que identificam uma rede sem fio.

Set Group ID Atributo de um arquivo (ou programa), normalmente utilizado em sistemas operacionais *Unix e Linux,* que indica que o arquivo deve ser executado com os mesmos direitos do grupo do arquivo, e não do usuário que o executou.

Set User ID Atributo de um arquivo, normalmente programa, utilizado em sistemas operacionais *Unix e Linux,* que indica que o programa deve ser executado com os mesmos direitos do dono do arquivo, e não com os do usuário que o executou.

Shadow Copies Cópia dos arquivos compartilhados em rede controlado por versão.

Shareware Programa de computador disponibilizado gratuitamente por um período determinado de tempo e muitas vezes com funcionalidades limitadas. Terminado o período de uso gratuito, normalmente o usuário é requisitado a pagar para acessar a funcionalidade completa.

Shutdown Processo de desligamento de um ativo.

Software Programa de computador.

Spam É o termo usado para referir-se aos *e-mails* não solicitados.

Spanning Tree Protocol Protocolo para equipamento de rede que permite resolver problemas de *loop* em redes comutadas.

Sticky bit Atributo especial de arquivo utilizado em sistemas operacionais *Unix* e *Linux* que antigamente era utilizado em determinados programas executáveis para informar ao sistema operacional que mantivesse uma imagem do programa em memória após o término do mesmo. Esta capacidade melhorava a resposta do sistema em chamadas subsequentes do programa pois eliminava a fase de carregamento do programa do disco. Esta característica era utilizada em programas grandes que demoravam muito para carregar ou em programas executados com muita frequência. O uso de modernas técnicas de memória virtual tornaram desnecessário o uso desta característica.

Switch Dispositivo utilizado em redes locais de computadores para encaminhar *frames* entre os diversos nós.

SYN *Flag* de um pacote TCP utilizado no processo de estabelecimento de uma conexão.

Syncookies Técnica utilizada para reduzir os efeitos de ataques do tipo *Synflood*.

Synflood É uma forma de ataque de negação de serviço na qual o atacante envia para o computador vítima uma grande quantidade de pacotes TCP de início de conexão (SYN) de forma a esgotar os recursos do sistema.

SYSKEY Utilitário usado para proteger a base de dados do SAM.

System Page File	Arquivo utilizado para armazenar páginas de memória RAM utilizada pelos processos que não estão em execução no momento.
Tabela ARP	Tabela que contém o mapeamento de endereços IP e endereços MAC.
Transmission Control Protocol / Internet Protocol	É um conjunto de protocolos de comunicação entre computadores em rede.
Terminal Service	Serviço do *Windows Server* que permite acessar um servidor ou computador remotamente.
Topologia da rede	*Layout* físico e o meio de conexão dos dispositivos da rede.
Uniform Resource Locator	Conjunto de caracteres utilizado para identificar um recurso disponível na *Internet*.
Universal Serial Bus	Permite a conexão de periféricos no computador.
Upload	É a transferência de dados de um computador local para um computador remoto.
Uniform Resource Locator	É um tipo de URI que indica onde um recurso está disponível e como ele deve ser acessado. Por exemplo a URL *http://kernel.org* indica que o serviço desejado deve ser acessado no servidor *kernel.org* usando o protocolo HTTP.
Virtual Local Area Network	Rede logicamente independente.
Vírus	Programa desenvolvido para alterar a forma como o computador opera, sem a permissão ou conhecimento do usuário. É capaz de se propagar, inserindo cópias de si mesmo e se tornando parte de outros programas.

Voice over Internet Protocol	Voz sobre IP (*Voice over Internet Protocol*). Roteamento de conversação humana usando a Internet ou qualquer outra rede de computadores baseada no Protocolo de Internet, tornando a transmissão de voz mais um dos serviços suportados pela rede de dados.
Vulnerabilidade	Falha em um sistema que pode ser explorada.
Web Application	Aplicação desenvolvida para o ambiente Web.
Wi-Fi Protected Access	Protocolo de segurança para redes sem fio desenvolvido para substituir o protocolo WEP devido às suas falhas de segurança.
Wireless	Rede sem fio.
Worm	Código malicioso que se dissemina criando cópias funcionais de si mesmo (ou de partes de si mesmo) em outros sistemas.

A ANEXOS

A.1 POLÍTICAS DE SEGURANÇA

A.1.1 Carta do Presidente

Mensagem do Presidente

Aos

Colaboradores e Prestadores de Serviço da M2FE

Ref: Política de Segurança da Informação (PSI) da M2FE

No cenário atual, no qual as empresas dependem cada vez mais das informações e de sistemas de informática para continuidade e competitividade dos negócios, é de vital importância direcionarmos ações visando garantir a segurança adequada das informações.

Assim, objetivando o melhor uso dos recursos de informação e adotando uma nova postura em relação à segurança da informação através de melhores práticas do mercado, está sendo oficializada a partir desta data a implantação de nossa Política de Segurança da Informação. Trata-se de um conjunto de documentos que valoriza e define o uso adequado dos recursos e das informações da empresa, evitando impactos na gestão dos negócios e possibilitando um ambiente de trabalho mais estável para a M2FE.

Precisamos trabalhar juntos para alcançar um alto padrão de segurança, em que todos sairão vencedores. Além dos incontáveis benefícios que trarão para a nossa empresa, estas políticas são fundamentais para a segurança de nosso ambiente.

Nesta data, fica instituído o Comitê de Segurança formado pelos seguintes colaboradores:

Nome	***Cargo/Função***	***Área***	***Telefones***	***Poder***
Funcionário4	Gestor do PCN	CSO	Telefone4	Decisão
Funcionário5	Gerente	Administrativo-Financeiro	Telefone5	Decisão
Funcionário6	Gerente	Produção e Assistência Técnica	Telefone6	Decisão
Funcionário7	Gerente	TI	Telefone7	Decisão

Estou certo que poderei contar com o apoio de todos e que a preocupação com as informações nos mais diversos níveis, será um compromisso individual dos profissionais que atuam na M2FE.

Campinas, 02 de Janeiro de 2009.

José da Silva

Presidente

A.1.2 Termo de responsabilidade, compromisso e sigilo

TERMO DE RESPONSABILIDADE, COMPROMISSO E SIGILO

NOME:_____

RG: _____

MATRICULA:_____

Eu, [*nome do colaborador*], pelo presente instrumento na condição de colaborador (a) da M2FE, comprometo-me a cumprir todas as especificações a seguir, em razão da permissão de acesso aos recursos necessários para a execução de minhas atividades profissionais, estando ciente, de acordo, e responsável.

1) É meu dever sempre zelar, cumprir e respeitar as políticas e procedimentos de segurança da M2FE, que regem o uso dos recursos a mim disponibilizados, sejam estes digitais ou impressos.

2) Quaisquer equipamentos ou informações, como identificador de usuário, senhas de acesso a sistemas, aplicativos, intranet, conta para acesso a correio eletrônico, crachás, chaves, *tokens* ou afins, que a M2FE me forneceu ou vier a me fornecer são individuais, intransferíveis, estarão sob minha custódia e serão utilizados exclusivamente no cumprimento de minhas responsabilidades funcionais.

3) Todos os acessos realizados e informações produzidas são passíveis de verificação e monitoração pela M2FE sem prévio aviso. A M2FE é a legítima proprietária de todos os equipamentos, infraestrutura e sistemas e informações disponibilizados para a execução do meu trabalho.

4) As informações por mim criadas ou recebidas durante a execução de minha função, dentro da jornada diária de trabalho, deverão tratar apenas de assuntos profissionais.

5) Não devo adquirir, reproduzir, instalar, utilizar e/ou distribuir cópias não autorizadas de softwares ou programas aplicativos.

6) Não é permitido o envio/saída de informações da M2FE, quer estas estejam em meios magnéticos (CDs, fitas, disquetes, *pen drives* etc) ou em meios físicos (papel, etc), ou até mesmo informações confidencias que tenho conhecimento sem a autorização de seu líder imediato.

7) Quando devidamente autorizado para acessar remotamente os recursos da M2FE para a execução de minhas atividades profissionais, devo manusear as informações obedecendo os mesmos critérios de segurança exigidos nas instalações internas.

8) Descumprindo qualquer um dos compromissos por mim assumidos neste Termo estarei sujeito às penalidades aplicáveis, como medidas administrativas e/ou disciplinares internas, e/ou ainda ações penais, cíveis ou trabalhistas previstas em lei.

_____ , ____ de _____ de _____.

_____

Assinatura do Colaborador

A.1.3 Diretrizes da Segurança da Informação

Garantir o atendimento das leis e normas que regulamentam as atividades da M2FE, de forma a obter aderência à legislação e regulamentações vigentes.

Assegurar que todos os usuários de ambientes e recursos de informações da M2FE tenham o dever de proteger contra a modificação, uso indevido, destruição, desvio, acesso ou divulgação não autorizada, garantindo sua integridade, confidencialidade e disponibilidade.

Garantir que as informações da M2FE tenham identificados seus proprietários, devendo este classificar as informações de forma segura e de maneira clara e objetiva.

Assegurar que quaisquer recursos e/ou Informações da M2FE somente sejam acessadas por usuários devidamente autorizados.

Assegurar que os Recursos de Segurança da Informação da M2FE sejam utilizados apenas para as finalidades lícitas, éticas e administrativamente aprovadas pela M2FE.

Garantir a monitoração do tráfego efetuado na M2FE, rastreando eventos críticos e evidenciando possíveis incidentes, dando ampla e geral divulgação dessa atividade e da possibilidade de uso desse recurso em caso de ocorrências.

Assegurar que o acesso físico às instalações de Segurança da Informação da M2FE seja feito seguindo os controles e registro de pessoas e equipamentos.

Assegurar que todos os usuários da M2FE estejam cientes das ameaças e das preocupações que possam intervir na segurança das informações da M2FE, e que sejam orientados para apoiar esta política.

Garantir a continuidade dos negócios de forma a reduzir a um período aceitável, qualquer eventual interrupção causada por desastres ou falhas de segurança, através da combinação de ações de prevenção e recuperação.

Assegurar a periódica análise dos processos e ativos de Informação da M2FE, de forma a identificar ameaças e vulnerabilidades de segurança.

Assegurar que os ativos da informação da M2FE estejam devidamente inventariados.

Assegurar que os sistemas e processos da M2FE tenham documentação adequada e suficiente para garantir seu entendimento e recuperação em casos contingenciais.

Prover auditorias periódicas, buscando a certificação do cumprimento dos requisitos de Segurança da Informação.

Deixar claro aos colaboradores, prestadores de serviço e estagiários que não é dado o direito de alegação de desconhecimento da Política de Segurança da Informação da M2FE, uma vez que a mesma é divulgada no âmbito interno da organização, devendo ser sempre seguida.

Garantir que a não observância dos preceitos deste documento implicará a aplicação de sanções administrativas previstas nas normas internas da M2FE.

Referências

- NBR ISO/IEC 27001:2006 (Sistemas de gestão de segurança da informação – Requisitos)
- NBR ISO/IEC 27002:2005 (Código de prática para a gestão da segurança da informação)

A.1.4. Políticas

A.1.4.1 Política de uso da Internet

Política Nº	*M2FE.001*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de uso da Internet

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por outrem, consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecerem as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de utilização segura da internet na M2FE com a finalidade de proteger os ativos de informação de sua propriedade contra ameaças externas ou internas, deliberadas ou acidentais.

A utilização de forma errônea da internet coloca em risco as informações e o negócio da empresa.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso da internet na organização.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra vazamentos, infecção por vírus, *worms* e/ou programas maliciosos, seja de forma acidental ou intencional.

5.1 Regras

O uso da *Internet* pelos colaboradores é permitido e encorajado desde que seu uso seja aderente aos objetivos e atividades fins do negócio da empresa e não comprometa o uso de banda da rede, nem perturbe o bom andamento dos trabalhos.

Os colaboradores poderão utilizar a internet para atividades não relacionadas com os negócios da empresa durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política e com a devida autorização de seu superior.

A M2FE se reserva no direito de bloquear, sem prévio aviso:

- Qualquer comunicação que apresente comportamento suspeito, ou por ordem expressa da administração;
- O acesso de qualquer usuário que infrinja qualquer uma das regras abaixo citadas;
- Acesso a arquivos ou domínio que comprometam o uso da banda Internet ou quaisquer recursos tecnológicos da Empresa;

Os colaboradores só devem utilizar programas, navegadores e comunicadores que foram homologados pelo departamento de Tecnologia da Informação.

Os colaboradores não devem clicar em *links* ou acessar sites desconhecidos que possam conter algum material prejudicial ou ofensivo à instituição e a outras pessoas.

Os colaboradores não devem acessar ou executar arquivos que contenham *plugins*, ActiveX ou quaisquer outros programas que adicionem funcionalidades a partir de sites desconhecidos;

É considerado inaceitável e passível das punições previstas nesta política, o uso da Internet para os seguintes fins:

- O acesso a sites que contenham conteúdo pornográfico, obsceno, racista, pedofilia, ou qualquer outro tipo de informação que possa causar constrangimentos.
- O envio de qualquer material que trata o item anterior, para outras pessoas, parceiros, empresas, instituições ou assemelhados mesmo com autorização das mesmas.
- Realizar *download* de quaisquer tipos de programa/*software (freeware* ou *shareware)* sem a prévia autorização do departamento de Tecnologia da Informação.

- Realizar *download* de *softwares,* materiais ou dados cujo direito pertença a terceiros (*copyright*), sem ter contrato de licenciamento ou outros tipos de autorizações.

- *Upload* de arquivos de qualquer software licenciado pela Empresa ou de dados de sua propriedade ou de seus clientes, sem expressa autorização do gerente responsável pelo software ou pelos dados.

- Acesso a *sites* que contenham material ilícito, bem como sua utilização para ataques e fraudes eletrônicas.

- Utilização de *sites* de relacionamento (Orkut, Myspace, Sonico...), jogos, passatempos, piadas, bem como quaisquer outros sites que tomem tempo desnecessário e não tenham relação direta com o trabalho realizado.

- Uso de programas de comunicação instantânea, *chat* e *VoIP* que não foram devidamente homologados pelo departamento de Tecnologia de Informação.

- Conversar e/ou trocar informações e arquivos em *chats* e grupos de discussão.

- Usar os recursos da M2FE para executar quaisquer tipos ou formas de atividades ilegais (tais como: fraudes, ou software/música pirata etc.).

- Atacar e/ou pesquisar áreas não autorizadas.

- Criar e/ou transmitir material difamatório.

- Executar atividades que desperdicem os esforços do pessoal técnico ou dos recursos da rede.

- Utilizar os recursos da empresa para deliberadamente propagar qualquer forma de vírus, *worms,* cavalos de tróia ou programas que controlem outros equipamentos.

- Falar e/ou escrever em nome da empresa para os meios de comunicação sem a devida autorização.

5.2 Monitoramento

A M2FE reafirma que o uso da *Internet* é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos funcionários e a própria reputação do negócio.

Os recursos tecnológicos da empresa existem para o propósito exclusivo de seu negócio. Portanto, a empresa se dá o direito de monitorar a utilização da Internet e da rede, juntamente com os endereços *web* (http://) visitados.

O não cumprimento da política resultará em sanções que variarão desde processos disciplinares, com avisos verbais ou escritos, até a demissão.

5.3 Responsabilidades

5.3.1 Usuários

Os usuários devem utilizar os recursos de acesso a ele disponibilizados com estrita observância da Política de Segurança.

Os usuários devem zelar pelo uso e acesso dos equipamentos sob sua responsabilidade, e responderão pelo acesso não autorizado e/ou mau uso dos equipamentos assim que tais atos sejam devidamente apurados.

Os usuários devem participar dos cursos e treinamentos de segurança da informação ora oferecidos pela M2FE.

Cabe aos usuários conhecer e executar todos os procedimentos relativos à política de segurança relacionados ao uso da internet na M2FE.

Em casos de dúvidas sobre o uso correto da Internet, o usuário deve solicitar esclarecimentos junto ao Comitê de Segurança. Este ato propiciará a melhora contínua das políticas.

5.3.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao Comitê de Segurança da Informação criar os mecanismos necessários à inspeção dos acessos à *Internet* quanto a desvios desta política.

Cabe ao departamento de Tecnologia da Informação definir as restrições de acessos a páginas internet.

5.4 Atribuições

O cumprimento desta política é obrigatória a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.5 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Cracker	Indivíduo que quebra um sistema de segurança, de forma ilegal ou sem ética.
Cavalos de tróia	Programa, normalmente recebido sob o pretexto de outro objetivo (por exemplo um cartão virtual), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas e sem o conhecimento do usuário.
Colaboradores	Funcionários, estagiários e prestadores de serviços.
Download	É a transferência de dados de um computador remoto para um computador local.
Freeware	É qualquer programa de computador cuja utilização não implica o pagamento de licenças de uso ou *royalties*.
Internet	Conglomerado de redes que interligam computadores em uma mesma rede, permitindo o acesso a informações e todo tipo de transferência de dados.
Intranet	O conceito é o mesmo da Internet, mas o acesso não é aberto, ou seja, apenas pessoas autorizadas podem acessar uma Intranet. Normalmente, é usada por empresas ou instituições para comunicação entre os colaboradores.
Home banking	Para se referir a serviço bancário doméstico via computador.
Shareware	É um programa de computador disponibilizado gratuitamente por um período determinado de tempo e muitas vezes funcionalidades limitadas. Terminado o período de uso gratuito, normalmente o usuário é requisitado a pagar para acessar a funcionalidade completa.
Upload	É a transferência de dados de um computador local para um computador remoto.
Vírus	Programa capaz de infectar outros programas e arquivos de um computador.

VoIP	Voz sobre IP.
Worm	Código malicioso que se dissemina criando cópias funcionais de si mesmo (ou de partes de si) em outros sistemas.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799:2005 - "Tecnologia da informação – Técnica de segurança - Código de Prática para Gestão da Segurança da Informação".

A.1.4.2 Política de uso do correio eletrônico

Política Nº	*M2FE.002*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de Uso do Correio Eletrônico

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de utilização segura do sistema de correio eletrônico na M2FE com a finalidade de proteger os ativos de informação de sua propriedade contra ameaças externas ou internas, deliberadas ou acidentais.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso do sistema de correio eletrônico da organização.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

5.1 Regras

O uso do correio eletrônico deve ser exclusivo para atividades relacionadas aos negócios da organização.

Somente deve ser utilizado software homologado pela M2FE no acesso ao correio eletrônico.

Cada usuário é responsável pela sua conta de correio eletrônico, não devendo ser compartilhada com nenhuma outra pessoa.

Mensagens de correio eletrônico (*e-mail*s) que contenham informações dos negócios da M2FE devem ser enviadas apenas aos proprietários dos negócios ou a destinatários autorizados a receberem tais informações.

As mensagens eletrônicas corporativas externas, enviadas e recebidas, que caracterizem o produto do trabalho, bem como as mensagens eletrônicas internas que constituam insumos

para os processos da organização, são consideradas informações corporativas e devem integrar o acervo documental da M2FE.

É proibida a distribuição de *e-mail*s com imagens de natureza pornográfica ou que contenham informações abusivas, racistas, constrangedoras, difamatórias ou quaisquer outras informações que possam denegrir a imagem da instituição ou de qualquer pessoa, seja de forma explícita (no corpo da mensagem) ou através de arquivos anexos.

É proibida a distribuição de *e-mail*s do tipo "corrente" ou quaisquer mensagens que aconselhem o destinatário da mensagem (o usuário) a repassar a mensagem para outros destinatários.

As mensagens recebidas com conteúdo proibido, conforme descrito nos itens anteriores, devem ser imediatamente apagadas.

É proibido o envio de *e-mail*s em nome de outrem.

A troca de mensagens entre colaboradores da M2FE contendo arquivos anexados deve ser evitada. Para a troca de arquivos, a forma preferencial deve ser a utilização das áreas de compartilhamento de arquivos disponíveis nos servidores da organização.

Toda mensagem originada na M2FE deve ser acrescida de texto explicativo indicando claramente a propriedade da mensagem e o seu uso correto, conforme a seguir:

"As informações contidas nesta mensagem e nos arquivos anexos são para uso exclusivo da M2FE, sendo seu sigilo protegido por lei. Caso não seja o destinatário desta mensagem, saiba que a sua leitura, divulgação, cópia e/ou qualquer forma de uso são proibidas. Portanto, favor apagar as informações e notificar o remetente. O uso impróprio será tratado conforme as normas da empresa e a legislação vigente."

Toda mensagem eletrônica (*e-mail*) criada ou armazenada usando-se recursos computacionais da empresa é de propriedade da M2FE.

A M2FE reserva-se o direito de acessar as mensagens eletrônicas de qualquer usuário, a qualquer momento, sem prévio aviso.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem utilizar os recursos de acesso a ele disponibilizados com estrita observância da Política de Segurança.

Os usuários devem zelar pelo uso e acesso dos equipamentos sob sua responsabilidade, e responderão pelo acesso não autorizado e/ou mal uso dos equipamentos assim que tais atos sejam devidamente apurados.

Os usuários devem participar dos cursos e treinamentos de segurança da informação ora oferecidos pela M2FE.

Cabe aos usuários conhecer e executar todos os procedimentos relativos à política de segurança relacionados ao uso do sistema de correio eletrônico da M2FE.

Em casos de dúvidas sobre o uso correto do sistema de correio eletrônico, o usuário deve solicitar esclarecimentos junto ao Comitê de Segurança. Este ato propiciará a melhora contínua das políticas.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao Comitê de Segurança da Informação criar os mecanismos necessários à inspeção das mensagens recebidas e enviadas quanto a desvios desta política.

Cabe ao departamento de Tecnologia da Informação definir e divulgar o tamanho da caixa postal de cada usuário.

É responsabilidade do departamento de Tecnologia da Informação providenciar os mecanismos de *backup* e recuperação das caixas postais de todos os usuários. A recuperação de mensagens das mídias de *backup* deve ser executada através de procedimento específico, a ser definido e divulgado pelo departamento de Tecnologia da Informação.

5.3 Atribuições

O cumprimento desta política é obrigatória a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Ameaça	Potencial de um agente da ameaça explorar uma vulnerabilidade específica, acidental ou intencionalmente.
Ativo	É qualquer bem que possua algum valor para a empresa.
Backup	Cópia de segurança.

Colaboradores	Funcionários, estagiários e prestadores de serviços
E-mail	Correio Eletrônico.
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.3 Política de uso de mídias removíveis

Política Nº	*M2FE.003*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de uso de mídias removíveis

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de utilização segura das mídias removíveis na M2FE com a finalidade de proteger os ativos de informação de sua propriedade contra ameaças externas ou internas, deliberadas ou acidentais.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso de mídias removíveis na organização.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

São consideradas mídias removíveis fitas, *flash disks*, discos removíveis, CDs, DVDs e mídias impressas.

5.1 Regras

A M2FE permite a utilização de mídias removíveis apenas se houver necessidade para o negócio da empresa.

Caso exista a necessidade de utilização de mídias removíveis por visitantes ou terceiros será necessária a abertura de um documento de exceção de política, o qual será enviado ao comitê de segurança da informação para avaliação e autorização.

Para utilização de mídias removíveis na M2FE é necessário preencher o formulário TI-047, disponível na Intranet, e levar a mídia removível ao departamento de TI para análise. A interface de preenchimento do formulário deve ser similar à apresentada na Figura 90.

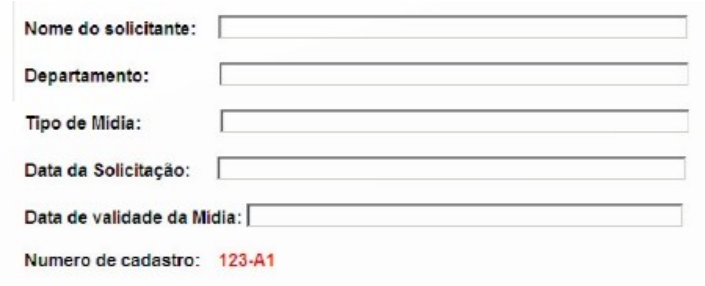


Figura 90: Modelo de interface

Caso seja autorizado o uso, as mídias removíveis serão cadastradas e etiquetadas pelo departamento de TI. Todas as mídias deverão ficar no cofre central da empresa e o seu acesso será controlado e restrito às pessoas autorizadas.

As etiquetas das mídias deverão possuir informações sobre o departamento que utiliza a mídia, o número de cadastro da mídia e prazo de validade da mesma, caso a mídia possua tempo de uso determinável, como é o caso de fitas magnéticas. Ao final desse prazo a mídia deve ser entregue ao departamento de TI para sua destruição.

Para realizar o descarte das mídias vencidas ou que não mais serão utilizadas, as mesmas deverão ser encaminhadas ao departamento de TI para serem destruídas. Todas as mídias descartadas deverão ser registradas, a fim de atender a auditoria.

Todas as mídias impressas deverão ser trituradas nas fragmentadoras.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem utilizar os recursos de acesso a ele disponibilizados com estrita observância da Política de Segurança.

Os usuários devem zelar pelo uso e acesso dos equipamentos sob sua responsabilidade, e responderão pelo acesso não autorizado e/ou mau uso dos equipamentos assim que tais atos sejam devidamente apurados.

Os usuários devem participar dos cursos e treinamentos de segurança da informação ora oferecidos pela M2FE.

Cabe aos usuários conhecer e executar todos os procedimentos relativos à política de segurança relacionados ao uso das mídias removíveis da M2FE.

Em casos de dúvidas sobre o uso correto do sistema de correio eletrônico, o usuário deve solicitar esclarecimentos junto ao Comitê de Segurança. Este ato propiciará a melhoria contínua das políticas.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao Comitê de Segurança da Informação criar os mecanismos necessários à inspeção da utilização segura das mídias removíveis ou desvios desta política.

É responsabilidade do departamento de Tecnologia da Informação providenciar e implementar os mecanismos necessários para o bloqueio de mídias removíveis não autorizadas.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.

- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.

- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Ameaça	Potencial de um agente da ameaça explorar uma vulnerabilidade específica, acidental ou intencionalmente.
Ativo	É qualquer bem que possua algum valor para a empresa.
Colaboradores	Funcionários, estagiários e prestadores de serviços.
Mídias removíveis	Fitas, *flash disks*, discos removíveis, CDs e DVDs.
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799:2005 - “Tecnologia da informação – Técnica de segurança - Código de Prática para Gestão da Segurança da Informação”.

A.1.4.4 Política de uso de dispositivos móveis

Política Nº	*M2FE.004*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de uso de dispositivos móveis

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de utilização de dispositivos móveis na M2FE com a finalidade de proteger os ativos de informação de sua propriedade contra ameaças externas ou internas, deliberadas ou acidentais.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso de dispositivos móveis nas dependências da organização.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

5.1 Regras

A concessão para uso de dispositivos móveis de propriedade da M2FE é permitida somente para atendimento de interesses da empresa.

O uso de dispositivos móveis somente deve ser concedido para colaboradores da M2FE e por absoluta liberalidade da empresa, para atendimento de necessidades profissionais específicas do colaborador perante a M2FE sendo legítima à empresa, a qualquer tempo e sem necessidade de prévio aviso ou justificativa, poder sem nenhum tipo de contestação:

- Solicitar ao colaborador a devolução imediata do equipamento.
- Restringir atividades identificadas como não sendo de interesse da M2FE.
- Monitorar e registrar as atividades efetuadas pelos colaboradores.
- Solicitar dos colaboradores justificativas pelas atividades realizadas.

Todo equipamento deverá ter uma placa de identificação patrimonial, e o colaborador deverá ter assinado o Termo de Responsabilidade e Sigilo (TRS) para receber junto com o recurso uma Declaração de Entrega do Equipamento.

Toda informação contida nos dispositivos móveis, bem como os softwares e aplicativos instalados, é propriedade da M2FE e deve ser protegida contra acessos indevidos, modificação, destruição ou divulgação não autorizada.

Toda concessão de dispositivos móveis da M2FE deverá ocorrer através de um pedido de solicitação de uso pelo Gestor imediato do colaborador, que será avaliado pela área de TI.

As solicitações de dispositivos móveis para uso temporário dos colaboradores da M2FE deverá ocorrer através de um pedido de solicitação de uso pelo gestor imediato do colaborador, remetido à área de TI devidamente justificado pela atividades a serem desenvolvidas, constando período e local de utilização.

A área de TI deve efetuar um teste de conformidade que garanta a integridade dos sistemas e ferramentas necessárias ao desenvolvimento das atividade do colaborador, bem como assegurar em sua devolução o perfeito estado do equipamento.

É expressamente proibida a alteração das configurações dos dispositivos móveis por parte do colaborador, bem como a instalação de softwares não homologados e licenciados pela M2FE.

A funcionalidade de gravação de CDs e/ou DVDs não deve fazer parte da configuração padrão dos equipamentos. Caso seja necessário, a liberação deve ser feita mediante autorização e justificativa do gestor imediato.

É expressamente proibido o acesso, exibição, edição, cópia, armazenamento e distribuição de material de conteúdo pornográfico e/ou que expressem ou promovam algum tipo de discriminação e/ou que não estejam de acordo com as finalidades designadas pela M2FE.

É expressamente proibida a instalação de dispositivos móveis pessoais, de propriedade de colaboradores, terceirizados, fornecedores e contratadas/os nas dependências da M2FE.

Todos os dispositivos móveis do tipo *notebooks* e similares em uso dentro do ambiente da empresa devem possuir um software antivírus instalado e atualizado para detectar, prevenir e eliminar a ocorrência de vírus, em suas diversas formas, automaticamente, sempre que possível. Cabe à área de TI definir formas para a detecção e instalação automática de antivírus nos recursos de computação móvel que se conectam à rede corporativa da M2FE.

Conexões às estações de dispositivos *handhelds*, dispositivos portáteis de armazenamento ou outros dispositivos capazes de armazenar informação são permitidas desde que estes sejam homologadas e de propriedade da M2FE.

Por ser um equipamento portátil e que, nem sempre, está conectado à rede, a dificuldade por manter cópias de segurança dos dados nele armazenados é grande. Portanto, para garantir a disponibilidade e integridade das informações, é responsabilidade do colaborador de posse do equipamento viabilizar com a área de TI uma agenda prévia de periodicidade mensal para a realização do *backup* das informações contidas no dispositivo.

Todos os arquivos críticos, sensíveis ou confidenciais devem permanecer na rede corporativa da M2FE, sendo responsabilidade do colaborador não manter estas informações em dispositivos móveis.

Especialmente no caso de *notebooks* a responsabilidade com relação à preservação da Segurança Física e Lógica, integridade, confidencialidade, disponibilidade, acesso e uso de ativos de informações da M2FE, é integralmente do colaborador que utiliza o equipamento, cabendo a todos:

- Comunicar toda e qualquer ameaça de apropriação indevida dos equipamentos, programas, periféricos ou informações à área de TI.

- Comunicar toda e qualquer vulnerabilidade identificada e pontos para melhoria da segurança das informações à área de TI.

- Tomar as devidas precauções ao utilizar este recurso em ambientes públicos, de forma a evitar o risco de captação de informações por pessoas não autorizadas ou roubo/furto do equipamento.

- Caso o equipamento venha a ser roubado ou furtado, cabe ao colaborador providenciar o boletim de ocorrência junto aos órgãos competentes da Polícia e com o boletim em mãos, comunicar imediatamente a Unidade de Segurança Patrimonial e a área de TI.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem utilizar os recursos a ele disponibilizados com estrita observância da Política de Segurança.

Os usuários devem zelar pelo uso e acesso dos equipamentos sob sua responsabilidade, e responderão pelo acesso não autorizado e/ou mau uso dos equipamentos assim que tais atos sejam devidamente apurados.

Todos os usuários que fazem uso temporário de dispositivos móveis devem estar cientes de suas responsabilidades através da assinatura de um termo específico e diferenciado, constando data de retirada, devolução e estado do equipamento. Em caso de danos ou necessidade de pequenos reparos será adicionado um comentário específico neste documento, com a ciência do colaborador.

Os usuários devem participar dos cursos e treinamentos de segurança da informação ora oferecidos pela M2FE.

Cabe aos usuários conhecer e executar todos os procedimentos relativos à política de segurança relacionada ao uso de dispositivos móveis da M2FE.

É responsabilidade do usuário de posse do equipamento viabilizar com a área de TI uma agenda prévia de periodicidade mensal para a realização do *backup* das informações contidas no dispositivo.

Todo usuário deve fazer uso das ações de conscientização proporcionadas pela M2FE, de forma de prevenção contra a infecção por programas maliciosos.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao Comitê de Segurança da Informação criar os mecanismos necessários à inspeção de cumprimento desta Política.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Ameaça	Potencial de um agente da ameaça explorar uma vulnerabilidade específica, acidental ou intencionalmente.
Ativo	É qualquer bem que possua algum valor para a empresa.
Backup	Cópia de segurança.
Colaboradores	Funcionários, estagiários e prestadores de serviços

Confidencialidade	Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.
Controle de acesso	Mecanismo que permite ou nega o acesso a um recurso.
Disponibilidade	Propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação, no momento em que for requisitada.
Dispositivo móvel	São pequenos dispositivos computacionais, tais como celulares e *notebooks*.
E-mail	Correio eletrônico.
Integridade	Propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição).
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.5 Política de senhas

Política Nº	*M2FE.005*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de senhas

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de criação e uso de senhas para uso em todos os sistemas homologados pela M2FE.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso dos sistemas computacionais da empresa.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

A política de senhas da M2FE é um instrumento importante para a proteção das informações da empresa. A senha consiste na primeira ferramenta que os usuários possuem para proteger suas informações e o fruto de seu trabalho na M2FE. Os usuários devem estar atentos para o fato de que as senhas são pessoais e intransferíveis e que, portanto, não devem ser divulgadas de forma alguma para outras pessoas, mesmo que colegas de trabalho.

5.1 Regras

Ao criar as suas senhas, os usuários devem observar as seguintes características e os sistemas não devem aceitar senhas que não estejam em conformidade com as mesmas:

- O tamanho mínimo da senha é de 8 caracteres.
- A senha deve conter, além de letras, pelo menos, dois números e dois símbolos.
- As senhas devem ser trocadas, no máximo, a cada 90 dias, sendo responsabilidade dos usuários efetuar a troca e dos sistemas de solicitarem-na, caso o usuário não o faça. Se

a senha não for trocada até o término do período estabelecido acrescido de 5 dias de tolerância, a conta de usuário deverá ser bloqueada.

- Os usuários não podem repetir nenhuma das últimas seis senhas utilizadas, e os sistemas devem garantir que esta premissa seja cumprida.

- Tentativas de acesso com senhas inválidas devem ser registradas e a conta de acesso deverá ser bloqueada após a quarta tentativa de acesso consecutivo sem sucesso. O desbloqueio só poderá ser efetuado pelo *help desk* da empresa mediante validação positiva do usuário.

A senha é pessoal e intransferível e, portanto, não deve ser compartilhada ou divulgada sob nenhuma circunstância.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem seguir as diretrizes para a criação de suas senhas.

Os usuários não devem fornecer as suas senhas a outros usuários, terceiros ou parceiros em nenhuma circunstância. Os usuários devem estar cientes de que todos os sistemas da empresa são protegidos por senhas e que apenas os usuários credenciados podem acessá-los. Se um usuário não tem a senha de acesso a algum sistema, é porque ele não está credenciado a usá-lo.

Cabe aos usuários conhecer e executar todos os procedimentos relativos à política de segurança relacionados ao uso correto de senhas.

Em casos de dúvidas sobre o uso correto de senhas, o usuário deve solicitar esclarecimentos junto ao Comitê de Segurança. Este ato propiciará a melhora contínua das políticas.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao departamento de Tecnologia da Informação manter os sistemas que permitam a definição ou troca de senhas em conformidade com as diretrizes definidas nesta política.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Senha	Frase, palavra-chave ou conjunto de caracteres utilizado para identificar o usuário ou sistema perante outro sistema, de forma a garantir-lhe ou não o acesso.

Colaboradores	Funcionários, estagiários e prestadores de serviços.
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.6 Política de *backup*

Política Nº	*M2FE.006*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de *backup*

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de *backup* da M2FE.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso dos sistemas computacionais da empresa e que, de alguma forma, produzirem dados ou informações que devam ser armazenadas para uso futuro.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

As cópias de segurança (*backup*) constituem um mecanismo de garantia de recuperação dos dados tanto em caso de desastres como em circunstâncias onde sejam necessárias informações que não estejam mais em uso operacional.

5.1 Regras

As cópias de segurança (*backup*) devem ser realizadas apenas nos servidores da empresa, não sendo efetuado nenhum tipo de cópia dos dados existentes nas estações de trabalho.

É responsabilidade do usuário copiar todos os dados de sua estação de trabalho e/ou *notebook* para os servidores da empresa.

A rotina de cópia de segurança é obrigatória e um sistema só pode ser colocado em operação quando dispuser dos procedimentos necessários para a realização das referidas cópias de segurança dos dados.

Os dados oriundos das cópias de segurança devem ser armazenados em fitas magnéticas ou mídias adequadas.

As cópias de segurança devem ser realizadas todos os dias, em mídias diferentes, que devem ser identificadas de acordo com o dia da semana e um número sequencial, que indica a ordem de gravação da mídia caso seja necessário mais de uma mídia por dia. É imprescindível que a cada dia da semana seja utilizado um jogo de mídias diferentes. Um jogo de mídias já utilizado pode ser reutilizado desde que as mídias estejam em bom estado e que não tenha sido atingido o limite máximo de uso, definido pelo fabricante.

Uma cópia completa dos dados deve ser realizada no último dia útil de cada mês e as mídias devem ser guardadas no cofre da empresa e/ou em local seguro fora da empresa. Esta cópia de segurança deve ser retida por 5 anos.

No último dia útil do ano é feito o *backup* anual que é guardado no cofre da empresa. Esse *backup* será retido por 5 anos.

Todas a mídias utilizadas devem ser testadas e todas as cópias de segurança devem ser verificadas e testadas, de forma a garantir a recuperação dos dados se necessário. A periodicidade de testes das cópias de segurança pode variar de acordo com o volume e sensibilidade dos dados, devendo ser definida junto aos responsáveis pelos dados e sistemas.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem armazenar **todos** os dados da empresa nos respectivos servidores. Todos os dados e informações pertinentes à M2FE devem ser sempre armazenados nos servidores.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao departamento de Tecnologia da Informação realizar as cópias de segurança e testá-las conforme descrito nesta política.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Backup	Cópia dos dados em outro local de forma que os mesmos possam ser recuperados em caso de desastre.
Colaboradores	Funcionários, estagiários e prestadores de serviços
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.7 Política de uso de *software*

Política Nº	*M2FE.007*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de uso de *software*

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores e parceiros. A segurança da informação tem por objetivo principal proteger o nome da organização, seus colaboradores e parceiros de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador e parceiro da M2FE. É responsabilidade de todos conhecer as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

A M2FE reconhece a importância do uso legal e ético de *software.* Este documento provê as regras que todos os colaboradores e terceiros devem seguir para garantir a utilização legal e ética dos *softwares.*

Todos os *softwares* são exclusivamente para uso relacionado ao negócio da empresa e não devem ser usados para interesses pessoais.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todas as áreas da organização, bem como prestadores de serviços, fornecedores, parceiros e todos os usuários que fizerem uso dos sistemas computacionais da empresa.

5 Política

A M2FE adquiriu licenças de uso para todos os *softwares* utilizados nos computadores e *notebooks* da empresa. Apenas programas autorizados e registrados são permitidos dentro da companhia bem como as cópias de *backup* apropriadas feitas conforme os acordos de licenciamento e políticas da empresa.

5.1 Regras

Fica expressamente proibida a cópia de qualquer *software* ou sua documentação sem a expressa autorização e consentimento do fabricante do *software* e da M2FE.

Software de outras origens

A M2FE proverá cópias de *software* legalmente adquirido para satisfazer todas as necessidades e em quantidades suficientes para todos os computadores da empresa. O uso de *software* obtido de qualquer outra fonte pode apresentar problemas legais para a M2FE além de apresentar uma ameaça à segurança computacional da empresa e, portanto, o uso de *software* não oficial é estritamente proibido.

Cópias adicionais

Os colaboradores da M2FE não poderão fazer cópia de qualquer programa ou documentação sem a autorização expressa do departamento de Tecnologia da Informação da M2FE.

Quando legal, a aprovação será concedida para tais instalações quando houver razões relacionadas ao negócio.

Cópias não autorizadas

A duplicação sem autorização de *software* registrado ou documentação é uma violação da lei e está fora dos padrões de conduta estabelecidos para um colaborador da M2FE. Usuários que adquiram ou usem cópias de software sem autorização estarão sujeitos às punições previstas nas penalidades desta política.

5.2 Responsabilidades

5.2.1 Usuários

Os usuários devem utilizar somente *softwares* homologados e disponibilizados pela M2FE.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao departamento de Tecnologia da Informação realizar auditorias periódicas em todos os computadores da empresa de forma a verificar conformidade com esta política.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Colaboradores	Funcionários, estagiários e prestadores de serviços
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.
Software	Programa de computador.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.8 Política técnica

Política Nº	*M2FE.008*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política técnica

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores. A segurança da informação tem por objetivo principal proteger o nome da organização e de seus colaboradores de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador da M2FE. É responsabilidade de todos conhecerem as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O objetivo desta política é estabelecer o padrão de informações técnicas, para serem configuradas em equipamentos, sistemas, aplicações, bem como serem obedecidas pelo corpo técnico da M2FE.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a toda área técnica da organização, bem como prestadores de serviços, fornecedores, parceiros e responsáveis pelas configurações técnicas dos sistemas computacionais da empresa.

5 Política

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

Este documento contém informações de caráter técnico que devem ser configuradas em todos os sistemas computacionais da organização a fim de garantir a confidencialidade, disponibilidade e integridade das informações da M2FE.

5.1 Regras

- O identificador de usuário (*login*) deve ser idealizado e padronizado, de forma que sirva no controle de acesso a recursos e na rastreabilidade de suas ações.
- Procedimentos operacionais devem ser documentados em um ponto único de armazenamento, mantidos em sigilo e atualizados. As mudanças destes procedimentos devem ser autorizadas pela área de TI.
- Dispositivos que façam varredura e/ou captura de dados trafegados nas redes corporativas (tais como *sniffers*) devem ter uso restrito, controlado, autorizado e limitado à área de TI.

- Os processos cíclicos de inventário dos recursos de informação da M2FE devem ser mantidos a fim de assegurar que as proteções estão sendo realizadas de forma efetiva.

- Os ativos inventariados devem seguir um padrão de identificação e incluir as informações necessárias que permitam à organização se recuperar de um desastre.

- Todos os recursos de TI da M2FE devem ser organizados e controlados de forma que possam, a qualquer momento e sem prévio aviso, ser vistoriados para ações preventivas de manutenção, controle e segurança. Esta norma se aplica inclusive a equipamentos portáteis próprios ou de terceiros que tenham sido autorizados para o uso nas atividades operacionais da organização.

- As correções dos sistemas operacionais, assim como os sistemas de navegação, correio eletrônico e pacotes de aplicativos devem ser implementadas após terem sido testadas e homologadas em ambiente apropriado.

- Os relógios dos servidores e equipamentos de conectividade devem estar sincronizados para garantir a exatidão dos registros de auditoria. Para facilitar o sincronismo dos relógios, é recomendado o ajuste periódico com um dispositivo UTC – *Universal Time Coordinated*.

- Para os processos terceirizados de Desenvolvimento de Sistemas, a área de TI deve acompanhar e controlar a homologação, implementação e/ou manutenção dos recursos *(hardware* e *software)* e/ou versões para o ambiente de produção de TI, através de um processo de gerência de mudanças.

- As mudanças em sistemas, aplicativos e pacotes devem ser formalmente aprovadas pelo gestor do sistema, comitê de segurança e pela área de TI.

- Toda inclusão, modificação e/ou exclusão nos sistemas, programas e aplicativos dos recursos de TI da M2FE deve ser documentada. Este preceito se aplica inclusive às mudanças de configuração, *upgrade* de sistemas, aplicativos e programas que possam de alguma forma, modificar o comportamento e/ou a desempenho de programas, sistemas, aplicativos, produtos e serviços.

- Para segregação e integridade das informações devem ser viabilizados ambientes distintos para desenvolvimento, homologação e produção. É obrigatória a existência de ambientes distintos de desenvolvimento, homologação e produção.

- Toda informação que seja considerada crítica aos negócios pelos seus proprietários e que requeira proteção e sigilo deve ser avaliada para que sejam aplicados mecanismos criptográficos adequados ou qualquer outra forma de recurso que garanta sua confidencialidade, integridade e disponibilidade.

- Os prestadores de serviços somente devem acessar as bases de dados no ambiente de desenvolvimento. Excepcionalmente, os prestadores de serviço poderão receber autorização temporária e controlada para acesso ao ambiente de homologação e produção, se devidamente justificado.

- O *Data Center* e ambientes onde estejam instalados servidores, equipamentos de conectividade e sistemas corporativos devem ser reservados e exclusivos, com acesso restrito, monitorado e controlado.

- Todos os recursos de TI da M2FE a serem disponibilizados em ambiente de produção, devem ser inventariados e previamente homologados em ambiente de testes.

- Todos os recursos de TI da M2FE devem estar protegidos pelo emprego de configurações adequadas de segurança em roteador, *firewall*, IDS/IPS (se disponível) e *proxy*. As configurações devem ser analisadas e testadas para levantamento e identificação e correção de vulnerabilidades, análise de invasão interna e análises externas.

- Os dados de configurações, topologia, análises e testes dos dispositivos do item anterior devem ser documentados para efeito de gestão do processo, controle e auditorias (internas e/ou externas).

- Todos os colaboradores da M2FE devem ser orientados sobre a forma adequada de uso dos equipamentos e dos aspectos de sua manutenção de forma que contribuam preventivamente na minimização de problemas e incidentes, e também para que saibam como agir no caso de alguma ocorrência.

- O acesso lógico aos recursos de TI somente será concedido mediante autorização do gestor imediato e da área de TI, com base em perfil previamente definido para o usuário de acordo com as funções e atividades de cada área, sendo vetada a criação de perfis não cadastrados para atendimento individual.

- Procedimentos e instruções de trabalho devem ser elaborados pelo departamento de TI com cuidados especiais para acesso remoto de colaboradores e terceiros aos sistemas e informações corporativas.

- O acesso remoto de contas administrativas deve estar limitado aos técnicos de TI e a situações eventuais e emergenciais, devendo ser monitorados quanto a esta utilização.

- Todo acesso remoto à M2FE deve ser feito através de aplicativos seguros com criptografia, níveis de acesso e avisos de segurança, sendo obrigatório que o acesso possua o recurso de *timeout* de forma que a sessão seja encerrada automaticamente caso não haja utilização dos recursos do sistema por um intervalo de tempo definido pela TI.

- Procedimentos e controles de acesso devem existir para conceder, bloquear, suspender e excluir acessos aos seus colaboradores, utilizando a conta de acesso com identificador único (ID) exclusivo e intransferível.

- Devem ser criados mecanismos entre as áreas de recursos humanos e TI de forma a possibilitar controle das movimentações de pessoal e direitos junto aos recursos tecnológicos.

- Controles devem ser implementados para assegurar que todo usuário ao acessar os recursos de TI tenha um único identificador, composto de conta *(login)* e senha, salvo situações especiais aprovadas em níveis adequados.

- A conta de acesso deve ser exclusiva, padronizada, pessoal, intransferível e ter uma senha sigilosa associada.

- Toda conta de acesso deve ter senha conforme Política **M2FE.005.**

- Conta com perfil de administrador deve ser restrita ao mínimo necessário e somente para colaboradores da área de TI ou sob autorização desta para casos formais e plenamente justificados.

- Devem existir controles para a configuração dos sistemas operacionais pela área de TI, com os devidos critérios de segurança e correções do fabricante.

- As estações de trabalho de TI devem ser bloqueadas automaticamente e seus aplicativos desconectados após 10 minutos de inatividade.

- As rotinas de *backup* estão contidas na política **M2FE.006**.

- Os recursos de TI da M2FE devem dispor de meios homologados para prevenção e combate a programas maliciosos (vírus, *spywares*, *trojans* etc).

- Toda função que aponte algum risco de segurança deve ser segregada e atribuída a mais de um responsável habilitado. Exemplo: conta especial com poder para alterar todas as configurações dos equipamentos não deve ter acesso à alteração de registros de auditoria e vice-versa.

- Todos colaboradores da M2FE que executem funções técnicas devem, durante a fase de recrutamento, assinar o Termo de Responsabilidade e Sigilo (TRS).

- Todo colaborador deve ser conscientizado quanto às Políticas de Segurança da Informação da M2FE (diretrizes, normas e procedimentos) e no uso correto e seguro de ambientes e recursos de TI da organização.

- Um processo de gestão de continuidade de negócios que permeie a infraestrutura, os ambientes e recursos de TI deve ser estabelecido, implantado e testado pela área de TI.

- Os planos de continuidade de negócio devem ser de conhecimento de todos, técnicos e colaboradores, de forma que possam ser entendidos e assimilados, considerando que por ocasião de contingências, têm que ser aplicados de maneira natural e efetiva.

- Qualquer incidente e/ou falha no esquema de segurança da informação deve ser comunicado imediatamente à área de Segurança da Informação.

- Todos os incidentes e/ou falhas de segurança da informação da M2FE devem ser registrados detalhadamente para análise oportuna.

5.2 Responsabilidades

5.2.1 Usuários

Respeitar as configurações implementadas, sem tentar burlar estas configurações em hipótese alguma.

5.2.2 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao departamento de Tecnologia da Informação, implementar as configurações em conformidade com as diretrizes definidas nesta política.

5.3 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.4 Penalidades

Todo desvio das disposições estabelecidas na presente política, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.

- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Senha	Frase, palavra-chave ou conjunto de caracteres utilizado para identificar o usuário ou sistema perante outro sistema, de forma a garantir-lhe ou não o acesso.
Colaboradores	Funcionários, estagiários e prestadores de serviços
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.1.4.9 Política de classificação da informação

Política Nº	*M2FE.009*	*Publicada em*	*02/01/09*
Assunto	*Políticas de Segurança da Informação*	*Validade*	*02/01/10*
		Versão	*1.1*

Política de classificação da informação

1 Introdução

A intenção da M2FE ao publicar suas políticas de segurança não é impor restrições à confiança depositada em seus colaboradores. A segurança da informação tem por objetivo principal proteger o nome da organização e de seus colaboradores de danos provocados por terceiros, sejam estes danos provocados consciente ou inconscientemente.

A segurança da informação só pode ser alcançada através do esforço contínuo de cada colaborador da M2FE. É responsabilidade de todos conhecerem as premissas e obrigações definidas nesta política e segui-las na condução de suas atividades.

2 Objetivo

O propósito desta política é ser um guia para a determinação do nível de segurança necessário para cada informação.

Classificação da Informação é o processo de identificar e definir níveis e critérios adequados de proteção das informações para garantir a confidencialidade, integridade e disponibilidade da informação de acordo com a sua importância para a M2FE.

Segundo o Item 7.2 da (NBR ISO/IEC 17799,2005), "*o objetivo da Classificação da Informação é assegurar que os ativos da informação recebam um nível adequado de*

proteção. A informação deve ser classificada para indicar a importância, a prioridade e o nível de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. Um sistema de classificação da informação deve ser usado para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento.”.

A observância e o cumprimento desta política são essenciais para que a missão da M2FE possa ser alcançada.

3 Vigência

Esta política passa a vigorar a partir da data de sua publicação.

4 Público Alvo

Esta política aplica-se a todos colaboradores da M2FE.

5 Política

5.1 Diretrizes

A Informação é o bem mais valioso da empresa e deve ser protegida contra alterações, divulgação não autorizada e/ou destruição, seja de forma acidental ou intencional.

5.2 Regras

Seguindo as recomendações de (WALLACE; WATKINS, 2008, p.15), as informações devem ser classificadas seguindo os critérios apresentados na Tabela 180 (Classificação da informação na M2FE). Para classificar as informações devem ser considerados o valor, a data de criação e a validade (ou tempo de vida útil) da informação.

Tabela 180: Classificação da informação da M2FE

Classificação	*Descrição*
Pública	Informação se torna disponível para o público, por exemplo, pelo *site* ou por materiais publicitários.
Sensível	Informação que pode causar constrangimento mas não ameaça a segurança se revelada.
Privada	Informação organizacional que deve ser mantida em segredo.
Confidencial	Informação sensível da organização que deve ser protegida com grande cuidado. Exemplo: informações de funcionários.

Na Tabela 181 (Atributos da informação) são definidos os atributos das informações.

Tabela 181: Atributos da informação

Atributo	*Significado*
Informação	Título ou nome que identifica a informação.
Formato	Formato da informação (fax, arquivo digital, carta etc).
Valor	Valor estimado da informação.
Data de criação	Data de criação da informação.
Validade (vida útil)	Tempo pelo qual a informação deve ser considerada relevante para a empresa, contado a partir da data de criação da mesma. Uma vez que a validade tenha expirado, a informação deve ser reclassificada.
Classificação	Nível de criticidade da informação.
Proprietário	Responsável pela informação (dono).

5.3 Responsabilidades

Os diferentes membros da organização devem assumir diferentes papéis para garantir o propósito da classificação e proteção da informação.

5.3.1 Proprietário da informação

É o responsável pela classificação do nível da informação conforme as regras estabelecidas nesta política.

Expirado o prazo de validade da informação, o proprietário da mesma deve reclassificá-la seguindo as regras estabelecidas nesta política.

5.3.2 Custódia da informação

O responsável pela custódia da informação é a área de TI.

É responsável pela manutenção das cópias de segurança e verificação da sua integridade.

É responsável pela restauração das cópias de segurança quando necessário.

Deve seguir as políticas e boas práticas para manter a classificação das informações.

5.3.3 Usuário

É responsável por usar as informações apenas para os propósitos da M2FE.

Deve tomar medidas de segurança necessárias para proteger a informação acessada.

5.3.4 Comitê de Segurança da Informação

É responsabilidade do Comitê de Segurança da Informação manter atualizada esta Política de Segurança.

Cabe ao departamento de Tecnologia da Informação, implementar as configurações em conformidade com as diretrizes definidas nesta política.

5.4 Atribuições

O cumprimento desta política é obrigatório a todos os envolvidos, conforme especificado no item *Público Alvo*. A não observância desta política está sujeita às penalidades descritas em item apropriado.

5.5 Penalidades

Todo desvio das disposições estabelecidas na presente norma, quando devidamente apurado, implicará:

- Aplicação de penalidades disciplinares previstas no regulamento pessoal dos colaboradores da M2FE.
- Aplicação das sanções previstas nos contratos de prestação de serviços e estágios, aos prestadores de serviço e estagiários.
- Aplicação das sanções previstas no Acordo de Sigilo assinado pelos fornecedores.

6 Glossário

Colaboradores	Funcionários, estagiários e prestadores de serviços
Política de Segurança da Informação	É um conjunto de diretrizes que têm por objetivo proteger a informação e disciplinar o seu uso.

7 Referências

Esta norma específica integra a Política de Segurança da Informação da M2FE e as Diretrizes Básicas da Organização, estando em consonância com a norma ABNT NBR ISO/IEC 17799 - “Código de Prática para Gestão da Segurança da Informação”.

A.2 PROCEDIMENTOS

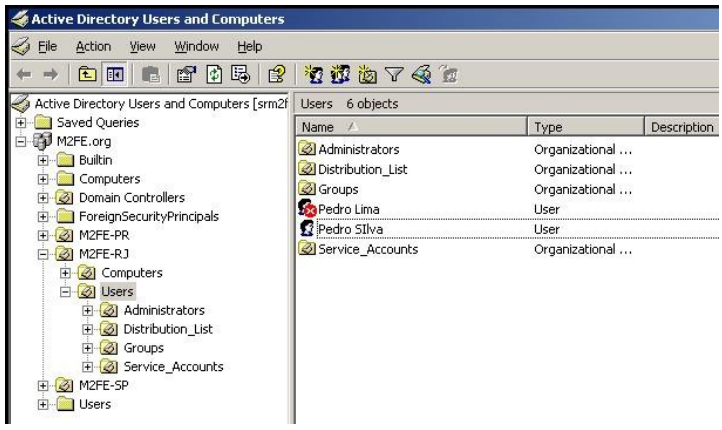
Com a finalidade de exemplificar procedimentos de segurança adotados pela M2FE apresentamos a seguir um procedimento relacionado à segurança da informação.

A.2.1 Procedimento de reconfiguração de senha de usuário

P-003: Reconfiguração de senha de usuário	
Responsável: João da Silva	**Código:** P-003
Descrição: Procedimento para reconfigurar a senha da conta de usuário no *Active Directory*.	
Sistema / Aplicação: Microsoft *Windows* 2003 *Server*.	

Histórico de alterações		
Data	***Responsável***	***Modificação***
25/07/2008	João da Silva	Criação do procedimento

Descritivo completo
Procedimento para reconfigurar a senha da conta do usuário. O motivo para ocorrer este bloqueio são: o usuário digitou mais de quatro vezes a senha errada, expiração da conta ou administrador pode ter desativado a conta enquanto o usuário estava de férias. Serão descritos todos os passos necessários para a ativação da conta do usuário no *Active Directory.*

Detalhamento da solução		
#	***O que fazer***	***Como fazer***
1	Abra o Gerenciador de usuários no *Active Directory*.	• Acesse o utilitário chamado *Active Directory Users and Computers*, o caminho é, clique em *Start* depois clique em *All Programs*, *Administrative Tool*, conforme ilustra a Figura 91.  **Figura 91: Utilitário de configuração de usuários**

Detalhamento da solução		
#	*O que fazer*	*Como fazer*
2	Selecione o usuário.	• Clique com o botão direito do *mouse* no nome da conta em que deseja reconfigurar a senha e em seguida escolha a opção *Reset Password*, conforme ilustra a Figura 92.

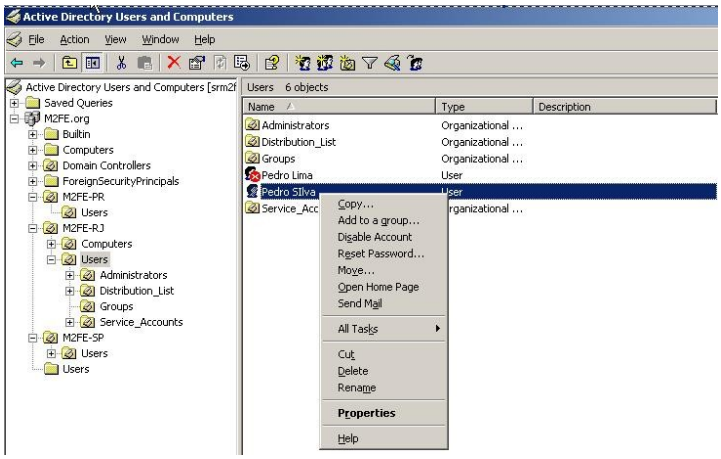
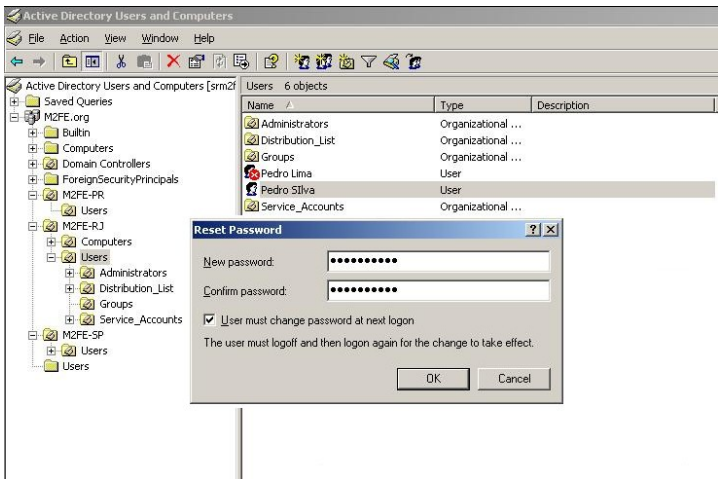
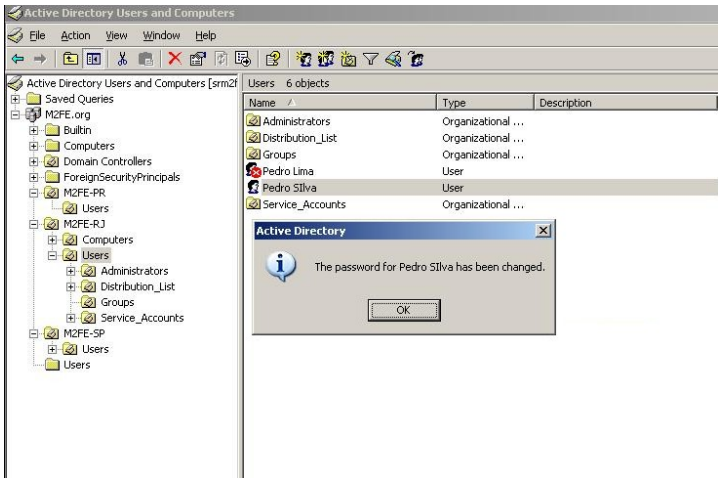


Figura 92: Troca de senha

Detalhamento da solução		
#	*O que fazer*	*Como fazer*
3	Digitar a nova senha temporária.	Digite e confirme a nova senha temporária seguindo a política de senha da M2FE que requer senha de no mínimo 8 caracteres contendo, além de letras, pelo menos dois números e dois símbolos. A opção *User must change password at next logon* deve ser selecionada pelo analista, conforme Figura 93.  **Figura 93: Troca de senha**

Detalhamento da solução		
#	***O que fazer***	***Como fazer***
4	Informe ao usuário a sua nova senha temporária.	• O analista de Help Desk verá a mensagem que a senha foi alterada com sucesso, conforme ilustra a Figura 94. Após visualizar esta mensagem o analista deve informar ao usuário a sua nova senha temporária informado que o sistema irá solicitar que ela seja trocada no próximo *login.*  **Figura 94: Mensagem de atualização de senha**
5	Encerrar o chamado.	• O analista deve encerrar o chamado no sistema de *Help Desk.*

A.3 PADRÕES DE SISTEMAS OPERACIONAIS

Na Tabela 182 são apresentados os sistemas operacionais avaliados pela M2FE. Os sistemas operacionais homologados contam com o suporte necessário da equipe de TI e podem ser adquiridos e utilizados normalmente na empresa. Os sistemas operacionais avaliados e não homologados não devem ser utilizados na empresa. Novos sistemas operacionais, isto é, aqueles ainda não avaliados, devem ser submetidos à avaliação e homologação antes de serem utilizados em ambiente de produção.

Tabela 182: Lista de sistemas operacionais avaliados na M2FE

Sistema Operacional	*Tipo de teste*	*Homologado*	*Comentários*
Microsoft Windows* Windows Server 2003 Enterprise Edition	Instalação e homologação	SIM	
Microsoft Windows* Windows 2003 Standard	Instalação e homologação	SIM	
Microsoft Windows XP Professional	Instalação e homologação	SIM	Service Pack 3
Red Hat Enterprise Linux 3.0	Instalação e homologação	NÃO	
Microsoft Windows 2000 Professional	Instalação e homologação	SIM	Service Pack 4
Microsoft Windows NT* 4.0 Server / Workstation	Instalação e homologação	NÃO	Descontinuado

Sistema Operacional	*Tipo de teste*	*Homologado*	*Comentários*
CISCO IOS	Testes básicos	SIM	Versões atualizadas
RedHat* Advanced Server 2.1	Teste básicos	NÃO	
Novell NetWare 5.1	Teste básicos	NÃO	
Microsoft Windows XP 64 Bits Professional	Instalação e homologação	SIM	
Linux Debian 4.0 (Etch)	Instalação e homologação	SIM	
Linux Debian 5.0 (Lenny)	Instalação e homologação	SIM	

A.4 MODELOS DE CHECKLISTS

A.4.1 Controles do *firewall Netfilter*

A Tabela 183 (*Checklist* de controles do *Firewall Netfilter*) apresenta a relação de controles a qual o *Firewall Netfilter* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DOMINGOS; MARUYAMA; MELO, 2006), (DERY, 2009), (SUEHRING; ZIEGLER, 2005) e (CISECURITY, 2007).

Tabela 183: *Checklist* de controles do *Firewall Netfilter*

Firewall Netfilter		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Versão do *Netfilter* deve ser a versão estável mais atual.	2	TEC						
2	Os registros de *log* do *Netfilter* devem ser analisados diariamente.	1	TEC						
3	Os arquivos de *log* devem ser rotacionados semanalmente.	2	TEC						

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
4	O *backup* das regras do *Netfilter* deve ser realizado semanalmente.	2	TEC						
5	As regras de filtragem devem ser criadas na ordem correta (e testadas).	8	TEC						
6	O endereço MAC do *gateway* da rede deve ser uma entrada estática na tabela ARP.	8	TEC						
7	Todas as regras do *Netfilter* devem usar endereços IP e não nomes.	8	TEC						
8	As regras antigas devem ser removidas no início da ativação do *Netfilter*.	8	TEC						
9	A filtragem de pacotes por estado (SPF) deve ser utilizada nas regras do *Netfilter*.	8	TEC						

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	O encaminhamento IP (IP Forward) deve ser desabilitado enquanto as regras do *Netfilter* não tiverem sido carregadas.	8	TEC						
11	Permitir tráfego de pacotes ICMP apenas para os tipos 0, 3, 8 e 11 (e*cho reply, destination unreachable, echo request* e *time exceeded*).	8	TEC						
12	As regras do *firewall* (*Netfilter*) devem ser revisadas semestralmente.	8	TEC						
13	Apenas tráfego explicitamente autorizado deve ser permitido entre a DMZ e a *intranet*.	1	TEC						
14	Procedimentos de configuração e instalação do *Netfilter* devem estar documentados.	2	TEC						

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
15	Pacotes com *flags* inválidas devem ser bloqueados.	2	TEC						
16	Pacotes mal formados devem ser bloqueados pelo *Netfilter*.	2	TEC						
17	As regras devem impedir a saída de pacotes da rede interna com IPs públicos.	1	TEC						
18	O *firewall Netfilter* deve ser instalado em um computador dedicado.	2	TEC						
19	Ferramentas gráficas de gerenciamento do *Netfilter* devem ser removidas.	1	TEC						
20	As permissões do arquivo de regras devem ser exclusivas ao usuário *root* (0600).	2	TEC						

Firewall Netfilter		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
21	As regras do *Netfilter* devem ser elaboradas de forma a registrar em *log* os eventos do tipo *critical*.	2	TEC						
22	As regras mais utilizadas devem ser posicionadas no início da tabela de regras do *Netfilter.*	2	TEC						
23	O uso da diretiva *any* nas regras do *Netfilter* deve ser evitado ou minimizado.	1	TEC						
24	O conjunto de regras do *Netfilter* deve possuir uma regra que rejeite o tráfego de pacotes do tipo *ident.*	1	TEC						
25	Possui equipamento de reserva?	8	TEC						

A.4.2 Controles do servidor de banco de dados

A Tabela 184 (*Checklist* de controles do servidor de banco de dados) apresenta a relação de controles a qual o servidor de banco de dados está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DISA, 2009).

Tabela 184: *Checklist* de controles do servidor de banco de dados

Servidor de banco de dados		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Versão do *software* deve ser a última disponível e compatível com o sistema.	10	TEC						
2	Aplicar as correções do banco de dados.	2	TEC						
3	A base de dados de desenvolvimento não deve conter dados de produção.	2	HUM						
4	O servidor deve ser dedicado.	2	TEC						
5	Usuários padrões de instalação devem ser removidos ou desabilitados.	1	TEC						

Servidor de banco de dados		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
6	Senhas criadas durante a instalação (*default*) devem ser substituídas.	1	TEC						
7	As contas dos usuários SYS e SYSTEM devem ser desabilitadas.	1	TEC						
8	Adotar o princípio de privilégio mínimo para as contas de usuários.	1	TEC						
9	Senhas de conexão ao banco de dados devem estar de acordo com a política.	2	TEC						
10	Remover os privilégios do grupo *PUBLIC*.	2	TEC						
11	Restringir a permissão *ANY* somente ao grupo de administradores.	1	TEC						
12	Parâmetro *remote_OS_authenticati on* em *FALSE*.	1	TEC						

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
13	Parâmetro *remote_login_passwordfile* em *EXCLUSIVE.*	1	TEC						
14	O *Listener* deve exigir autenticação nas conexões.	9	TEC						
15	Acesso físico ao servidor deve ser restrito e controlado.	6	TEC						
16	Desabilitar ou restringir os dispositivos de armazenamento (fita, CD, USB).	1	TEC						
17	A restauração do banco de dados deve ser restrita e autorizada aos administradores.	1	HUM						
18	Dados armazenados em *backup* devem ser cifrados.	1	TEC						
19	O serviço DBSNMP deve estar desabilitado.	2	TEC						

Servidor de banco de dados		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
20	Deve haver procedimento para verificar a liberação de novas correções.	10	TEC						
21	O acesso remoto (*Terminal Service*) deve ser restrito e controlados aos administradores.	1	HUM						
22	O tráfego de dados do banco de dados na rede deve ser cifrado.	2	TEC						
23	Não permitir acesso de analistas aos dados de produção.	11	TEC						
24	Bloquear a execução de DDL para o usuário de conexão da aplicação.	2	TEC						
25	Os arquivos de *trace* só devem ser acessíveis pelo DBA.	11	TEC						

A.4.3 Controles do servidor ERP

A Tabela 185 (*Checklist* de controles do servidor ERP) apresenta a relação de controles a qual o servidor ERP está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DISA, 2007).

Tabela 185: *Checklist* de controles do servidor ERP

Servidor ERP		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	O banco de dados do ERP não pode ser compartilhado com outras aplicações.	2	HUM						
2	As senhas não devem ser armazenadas pelo sistema, apenas o *hash* das mesmas.	2	TEC						
3	Todos os arquivos da aplicação ou criados pela mesma devem estar protegidos de acessos não autorizados.	2	TEC						
4	As mudanças devem ser analisadas e aprovadas antes da sua implementação.	11	HUM						

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Documentar os controles de segurança, responsabilidades e procedimentos.	11	HUM						
6	O controle de acesso da aplicação deve ser baseado em segregação de funções.	2	TEC						
7	Somente os responsáveis pela segurança poderão liberar acesso aos usuários.	11	HUM						
8	O acesso à informação, bens e recursos devem ser restritos somente aos usuários autorizados.	2	TEC						
9	As contas de usuários inativos devem ser desabilitadas.	2	TEC						
10	Os procedimentos de atualização de *software* devem estar documentados.	11	HUM						

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
11	Garantir que os desenvolvedores não tenham acesso ao ambiente de produção.	11	TEC						
12	Todas as ações dos usuários devem ser registradas em *log* (trilha de auditoria).	1	TEC						
13	As contas de usuários devem ser desativadas após 3 tentativas consecutivas de acesso sem sucesso.	1	TEC						
14	Adotar o princípio de privilégio mínimo para as contas de usuário.	1	TEC						
15	A comunicação entre a aplicação e o banco de dados deve ser cifrada.	2	TEC						
16	O código da aplicação não deve ser mantido junto com a aplicação.	11	HUM						

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
17	Os recursos de rede (IP, URL etc), chaves e senhas não podem ser *hardcoded.*	11	HUM						
18	Os arquivos de *log* devem ser rotacionados semanalmente.	8	TEC						
19	As atividades dos administradores devem ser registradas em *log* e monitoradas.	8	TEC						
20	Deve ser emitido aviso quando os *logs* estiverem a 80% da capacidade de saturação.	1	TEC						
21	Qualquer ferramenta de auditoria devem ser de uso restrito aos auditores.	2	TEC						
22	Verificar semestralmente se os *user IDs* são válidos, aprovados e com segregação de funções (auditoria).	11	HUM						

Servidor ERP		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Nenhuma conexão anônima deve ser permitida pela aplicação.	9	TEC						
24	Revisar semestralmente as regras de acesso para garantir que nenhuma regra tenha sido alterada.	11	HUM						

A.4.4 Controles do servidor *Windows* 2003 *Active Directory*

A Tabela 186 (*Checklist* de controles do servidor *Windows Active Directory*) apresenta a relação de controles a qual o servidor *Windows Active Directory* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DISA, 2009).

Tabela 186: *Checklist* de controles do servidor *Windows Active Directory*

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
1	Habilitar complexidade de senhas na política de domínio conforme a política da empresa.	1	TEC						
2	Habilitar política de histórico das últimas 5 senhas na política de domínio.	1	TEC						
3	Habilitar o requisito mínimo de 8 caracteres para todas as senhas das contas dos domínios.	1	TEC						
4	Habilitar o requisito minimo de 15 caracteres para todas as contas administrativas.	1	TEC						

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Restringir o acesso remoto aos servidores Controladores de Domínio aos administradores.	1	TEC						
6	Documentar todos servidores *Active Directory* e Global *catalog.*	2	TEC						
7	Documentar o FSMO (regras do domínio).	2	TEC						
8	Garantir que todos os A*ctive Directories* estão sincronizados.	10	TEC						
9	Proteger o acesso ao *Active Directory Schema Master* de acesso não autorizado.	1	TEC						
10	Possuir pelo menos 2 servidores controladores de domínio trabalhando ativamente.	10	TEC						

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
11	Garantir que os servidores de *Active Directory* são dedicados para esta função.	10	TEC						
12	As contas de serviço devem possuir nomes longos, com alta complexidade de senhas e não podem expirar.	1	TEC						
13	Garantir que os administradores possuem contas separadas para as atividades diárias e outra para as administrativas.	2	TEC						
14	Executar diariamente o *backup* da SAM e do *Schema Master*.	2	TEC						
15	Utilizar o serviço de DNS integrado ao *Active Directory* apenas para *hosts* internos (do domínio).	10	TEC						

Windows Active Directory		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
16	Possuir ao menos 2 servidores habilitados com *Global Catalog* na Floresta.	10	TEC						
17	Utilizar serviço NTP para sincronização de data e hora para todos os servidores.	10	TEC						
18	Documentar procedimento de promoção e remoção de controladores de domínios.	11	TEC						
19	Garantir que todas as atualizações de segurança sejam instaladas.	1	TEC						

A.4.5 Controles do servidor de arquivos *Windows* 2003

A Tabela 187 (*Checklist* de controles do servidor de arquivos *Windows* 2003) apresenta a relação de controles a qual o *servidor de arquivos Windows 2003* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DISA, 2009).

Tabela 187: *Checklist* de controles do servidor de arquivos *Windows* 2003

Servidor de arquivos		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Todos os compartilhamentos devem ser documentados.	2	TEC						
2	Todos os compartilhamentos devem ser ocultos.	1	TEC						
3	O mapeamento dos compartilhamentos deve ser feito via VB *Script*.	2	TEC						
4	Garantir que o IIS não esteja instalado no servidor.	2	TEC						
5	A estrutura de pastas deve seguir o organograma da empresa.	2	TEC						

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	O diretório *home* de cada usuário deve ter acesso restrito ao usuário proprietário do diretório.	2	TEC						
7	Deve ser configurado uma quota de 1GB por usuário.	10	TEC						
8	O conteúdo do diretório público da rede deve ser apagado diariamente às 00h00.	2	TEC						
9	Documentar todas as unidades mapeadas, conforme sua função.	2	TEC						
10	Deve ser fornecida área cifrada para armazenamento de arquivos classificados como confidenciais.	2	TEC						
11	Garantir que o grupo *everyone* (todos) seja removido de todos os compartilhamentos.	2	TEC						

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Garantir que esteja sendo cumprida a política de *backup*.	2	TEC						
13	Garantir que os arquivos compartilhados estejam em uma partição diferente da utilizada pelo sistema operacional.	2	TEC						
14	Garantir que este servidor seja exclusivo para compartilhamento de arquivos.	10	TEC						
15	Garantir que todos os arquivos de trabalho sejam gravados no servidor.	2	TEC						
16	Habilitar o recurso de *Shadow Copies* no volume onde os compartilhamentos estão criados.	2	TEC						

Servidor de arquivos		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
17	Configurar o *Shadow Copies* para executar todos os dias da semana às 10h00 e às 15h00.	2	TEC						
18	Limitar o tamanho do *Shadow copies* para 20GB.	2	TEC						
19	Auditar bimestralmente a conformidade de permissões com as definidas pela diretoria.	2	TEC						

A.4.6 Controles do *data center*

A Tabela 188 (*Checklist* de controles do *data center*) apresenta a relação de controles a qual o *data center* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações obtidas em (HARRIS, 2007).

Tabela 188: *Checklist* de controles do *data center*

Data center		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Remover do interior do *data center* todos os materiais não relacionados às atividades do mesmo.	11	HUM						
2	Instalar filtros de limpeza ou contra gases e vapores.	7	TEC						
3	Deve existir um termostato exclusivo para controle de temperatura do *data center.*	10	TEC						
4	Deve ser definido e instalado um sistema de refrigeração de contingência para o *data center.*	4	TEC						

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	O sistema de refrigeração do *data center* deve ser exclusivo.	4	TEC						
6	Devem ser elaborados registros de manutenção preventiva do sistema de ar condicionado.	4	TEC						
7	Instalar câmeras de CFTV externas e internas ao *data center* e armazenar as imagens por 180 dias.	1	TEC						
8	Não permitir o acesso de visitantes ao *data center* sem prévia autorização da segurança e sem acompanhante.	1	HUM						
9	A porta do *data center* deve ser provida de mecanismo de fechamento automático.	1	TEC						

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	Os circuitos elétricos do *data center* devem ser divididos e dimensionados adequadamente.	10	TEC						
11	Devem ser instalados circuitos elétricos com tomadas suficientes para o *data center*.	8	TEC						
12	Devem ser instaladas pelo menos duas unidades de luz de emergência no interior do *data center*.	8	TEC						
13	A tensão de alimentação dos equipamentos do *data center* deve ser estabilizada.	8	TEC						
14	Devem ser instalados *no-breaks* para os equipamentos críticos do *data center*.	8	TEC						

Data center		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
15	Não deve haver nenhuma identificação da localização do *data center.*	1	HUM						

A.4.7 Controles da rede

A Tabela 189 (*Checklist* de controles da rede) apresenta a relação de controles a qual a rede está sujeita.

Tabela 189: *Checklist* de controles da rede

Rede		***Tipo ameaça***	***Tipo vuln.***	***Implementado***	***Custo estim. (HH)***	***Investimento estim. (R$)***	***Prob.***	***Impacto***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	O endereçamento IP utilizado na LAN é privado (RFC1918).	8	TEC						
2	O cabeamento de rede é certificado.	8	TEC						
3	Devem ser utilizadas fibras ópticas com redundância entre os *switches* de distribuição e o *Core.*	8	TEC						
4	A topologia da rede deve ser estruturada em formato *full mesh* (redundância).	8	TEC						
5	O protocolo STP deve estar habilitado e configurado corretamente.	8	TEC						

Rede		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	A rede deve ser segmentada.	8	TEC						
7	Deve ser utilizado *switch core* L3 com redundância.	8	TEC						
8	Devem ser Implementadas *Access Control List*s entre VLANs.	8	TEC						
9	Deve haver *firewall* entre as VLANs.	8	TEC						
10	Deve haver IPS em todos os segmentos da LANs.	8	TEC						
11	NAC está implementado	8	TEC						
12	Utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory*.	8	TEC						

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
13	Deve ser utilizado protocolo de roteamento autenticado.	8	TEC						
14	Deve haver sumarização de rotas.	8	TEC						
15	Os *links* de dados através da WAN devem ser cifrados.	8	TEC						
16	Deve haver *switches* de reserva.	10	TEC						
17	Os *racks* de distribuição devem possuir ventilação adequada.	8	TEC						
18	Os cabeamentos estruturados devem ser separados dos cabeamentos elétricos	8	TEC						
19	A função *anti-snooping* deve ser habilitada nos *switches*.	8	TEC						

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
20	O servidor DNS deve estar configurado conforme orientação do fabricante.	8	TEC						
21	O parâmetro de atualização dinâmica de zona deve estar habilitado no servidor (Windows).	8	TEC						
22	O DNS deve estar integrado ao *Active Directory*.	8	TEC						
23	O IPSEC deve estar configurado na comunicação entre o ERP e o banco de dados.	8	TEC						
24	Deve ser desativada a *community public* do SNMP.	8	TEC						
25	A rede sem fio não deve propagar o SSID.	8	TEC						

Rede		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
26	O filtro de endereços MAC deve estar habilitado na rede sem fio.	8	TEC						
27	A criptografia da rede sem fio deve estar no modo WPA2.	8	TEC						
28	Todo dispositivo sem fio deve utilizar método de autenticação 802.1x com o serviço IAS do *Windows* 2003 integrando toda a autenticação ao *Active Directory*.	8	TEC						
29	Os *firmwares* de todos os ativos de rede devem estar atualizados para a última versão.	8	TEC						
30	O sinal da rede sem fio não deve propagar além do perímetro físico da empresa.	8	TEC						

Rede		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
31	A conexão com dispositivos de rede sem fio deve ser desativada após 15 minutos sem uso.	8	TEC						
32	Todos os ativos de rede devem ter as senhas padrão alteradas.	8	TEC						
33	Garantir que o ponto de acesso está em local seguro.	4	TEC						
34	Serviços acessíveis externamente devem estar na DMZ.	8	TEC						
35	O *Port Security* deve estar habilitado nos *switches*.	8	TEC						
36	Deve haver um servidor de DHCP *backup* para distribuição de endereçamento IP.	8	TEC						
37	Garantir que não existam *links* externos não gerenciados.	8	TEC						

A.4.8 Controles de segurança física

A Tabela 190 (*Checklist* de controles da segurança física) apresenta a relação de controles a qual a segurança física está sujeita. Os itens deste *checklist* foram elaborados com base nas informações obtidas em (HARRIS, 2007).

Tabela 190: *Checklist* de controles da segurança física

Segurança física		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	O perímetro externo da empresa deve ter cerca com altura igual ou superior a 2,5 metros.	1	HUM						
2	Deve haver sensores de invasão no perímetro da empresa.	1	HUM						
3	Deve haver guarda patrimonial 24 horas por dia.	1	HUM						
4	O perímetro externo da empresa deve possuir placa de aviso de propriedade privada.	1	HUM						
5	Deve haver cães de guarda treinados.	1	HUM						

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
6	Deve existir sistema de detecção e combate a incêndio.	1	AMB						
7	As áreas criticas devem possuir controle de acesso.	1	TEC						
8	Devem ser elaborados registros de manutenção preventiva do sistema de alarme.	4	HUM						
9	Deve haver câmeras de CFTV externas e internas e as imagens devem ser retidas por 180 dias.	1	HUM						
10	A brigada de incêndio deve ser treinada anualmente.	1	HUM						
11	Todos os painéis de distribuição devem ser trancados.	1	HUM						

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
12	Os circuitos elétricos devem ser divididos e dimensionados adequadamente.	10	TEC						
13	Devem ser instalados pára-raios para a proteção dos equipamentos e do prédio.	7	AMB						
14	Deve haver uma malha de aterramento elétrico para os equipamentos elétricos e eletrônicos.	8	AMB						
15	Todas as eletro-calhas e tubulações metálicas devem ser aterradas.	8	AMB						
16	O grupo moto-gerador deve ser testado mensalmente.	8	TEC						
17	Devem ser instaladas unidades de luz de emergência no interior da empresa.	8	TEC						

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Todos os circuitos elétricos devem ser protegidos por disjuntores termomagnéticos.	8	TEC						
19	Todos os circuitos elétricos devem ser identificados com etiquetas legíveis.	8	HUM						
20	Deve ser elaborado um mecanismo de registro de incidentes de segurança física.	11	HUM						
21	Todos os visitantes devem ser devidamente identificados, registrados e portar crachá em local visível.	4	AMB						
22	O sistema de alarme de incêndio deve ser testado mensalmente e o teste deve ser registrado.	4	TEC						

Segurança física		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
23	Os extintores de incêndio devem ser inspecionados trimestralmente (com registro).	4	TEC						
24	O cabeamento deve ser verificado quanto à conformidade com as normas de cabeamento estruturado.	10	TEC						
25	Todos os cabos devem ser devidamente identificados.	10	TEC						
26	Os cabeamentos de dados, telefonia e de energia elétrica devem ser instalados fisicamente separados.	8	TEC						
27	Os cabos de dados do *data center* devem ser instalados diretamente (ponto-a-ponto) sem emendas.	8	TEC						

Segurança física		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
28	Os dutos de ar condicionado devem ser revestidos externamente por material térmico e não combustível.	4	TEC						
29	Os equipamentos de refrigeração instalados externamente devem ser devidamente protegidos contra acesso físico não autorizado.	1	TEC						
30	Os vidros da guarita de entrada devem ser escuros ou cobertos com película protetora escura.	1	AMB						

A.4.9 Controles do sistema operacional *Windows* 2003 *Server*

A Tabela 191 (*Checklist* de controles do sistema operacional *Windows* 2003 Server) apresenta a relação de controles o sistema operacional *Windows 2003 Server* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DISA, 2009).

Tabela 191: *Checklist* de controles do sistema operacional *Windows* 2003 *Server*

Controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Verificar se todas partições estão formatadas com NTFS.	2	TEC						
2	Permitir apenas a instalação de dispositivos com *drivers* assinados digitalmente.	2	TEC						
3	Desabilitar os compartilhamentos padrões (C$, IPC$ e ADMIN$).	2	TEC						

Controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
4	Garantir que os *logs* de eventos sejam configurados de forma que quando atingirem 160MB seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC						
5	Remover todos os compartilhamentos não documentados.	2	TEC						
6	Definir as permissões de compartilhamento e NTFS seguindo a classificação da informação.	1	TEC						
7	Remover o acesso anônimo aos compartilhamentos.	1	TEC						
8	Garantir que o *firewall* local do sistema esteja habilitado.	9	TEC						
9	Permitir autenticação somente em NTLMv2.	1	TEC						

Controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
10	Garantir que a auditoria esteja habilitada.	1	TEC						
11	Garantir que seja desabilitado, a enumeração anônima da base de dados SAM.	1	TEC						
12	Desabilitar a conta *guest.*	1	TEC						
13	Renomear a conta do administrador.	1	TEC						
14	A versão mais atual do componente *Microsoft DirectX* deve estar instalada.	9	TEC						
15	O parâmetro do registro *RunAs* deve ser removido de todas as sub-chaves da chave *HKLM\Software\Classes\ AppID.*	2	TEC						
16	Desabilitar a conta de usuário *SUPPORT_388945a0*, utilizada para suporte da Miscrosoft.	1	TEC						

Controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
17	As informações classificadas como críticas devem ser armazenadas de maneira cifrada.	2	TEC						
18	Desabilitar o *autorun* de todos os *drives*.	2	TEC						
19	Garantir que todas as correções de segurança disponibilizadas pelo fabricante estejam instaladas.	2	TEC						
20	Instalar anti-vírus e configurar de forma que seja atualizado diariamente.	2	TEC						
21	Habilitar a notificação automática de novas correções críticas disponíveis.	2	TEC						

Controles do sistema operacional Windows 2003 Server		*Tipo ameaça*	*Tipo vuln.*	*Implementado*	*Custo estim. (HH)*	*Investimento estim. (R$)*	*Prob.*	*Impacto*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
22	As permissões NTFS para o diretório *%SystemRoot%* devem ser configuradas de forma a permitir acesso apenas ao grupo Administradores.	1	TEC						
23	Garantir que o *backup* siga as especificações da política de *backup.*	2	TEC						
24	Garantir que o *Windows 2003 Server* seja configurado para enviar um *e-mail* para o administrador quando ocorrer qualquer evento do tipo ERRO.	10	TEC						
25	O recurso de geração do arquivo de DUMP da memória deve ser desabilitado.	2	TEC						
26	O licenciamento do *Windows* 2003 *Server* deve ser respeitado.	11	TEC						

Controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
27	Habilitar o SYSKEY (solicitação de senha para carregamento da base de dados SAM na inicialização do sistema).	2	TEC						
28	Garantir que as configurações de rede estejam documentadas.	11	TEC						
29	Configurar a proteção contra ataques SYN.	9	TEC						
30	Configurar o número máximo de retransmissão de pacotes SYN para 3.	9	TEC						
31	Os *logs* de eventos devem ser verificados diariamente.	2	TEC						
32	Não armazenar as credenciais de autenticação e/ou do .NET *passports*.	1	TEC						
33	Os *hashes* das senhas do LAN Manager não devem ser armazenados no SAM.	1	TEC						

Controles do sistema operacional Windows 2003 Server		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
34	O desempenho do *Windows 2003 Server* deve ser monitorado semanalmente.	8	TEC						
35	Desabilitar o botão de *shutdown* do servidor.	2	TEC						
36	Habilitar a exclusão do *System Page File* na inicialização do sistema.	2	TEC						
37	O sistema não deve permitir o suporte remoto não solicitado.	1	TEC						
38	Garantir que, quando o arquivo de auditoria atingir 160MB, seja emitido um aviso (*e-mail* ou similar) ao administrador.	10	TEC						
39	Desabilitar a instalação automática de qualquer componente do *Windows*.	2	TEC						

Controles do sistema operacional Windows 2003 Server		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
40	Garantir que o disco de reparo de emergência do *Windows* esteja atualizado.	8	TEC						

A.4.10 Controles do Sistema Operacional Linux

A Tabela 192 (*Checklist* de controles do sistema operacional Linux) apresenta a relação de controles o sistema operacional *Linux* está sujeito. Os itens deste *checklist* foram elaborados com base nas informações apresentadas em (DOMINGOS; MARUYAMA; MELO, 2006), (DERY, 2009), (SUEHRING; ZIEGLER, 2005) e (CISECURITY, 2007).

Tabela 192: *Checklist* de controles do sistema operacional Linux

Controles do sistema operacional Linux		***Tipo ame-aça***	***Tipo vuln.***	***Imple-men-tado***	***Custo estim. (HH)***	***Investi-mento estim. (R$)***	***Prob.***	***Im-pac-to***	***Risco***
#	***Controle***						***Nível***	***Nível***	***Nível***
1	Instalar as correções de segurança sempre que disponibilizadas pelo fabricante.	9	TEC						
2	Desabilitar os privilégios SUID e SGID dos programas não essenciais à função do servidor.	9	TEC						
3	Desabilitar o serviço *portmap* se o servidor não utilizar NFS.	9	TEC						
4	Limitar o número de processos que um usuário pode executar simultaneamente.	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
5	Remover os serviços não necessários para a função do servidor (FTP, DNS, Apache etc).	9	TEC						
6	Desabilitar o acesso da conta root nos consoles locais.	9	TEC						
7	Criar contas com privilégios mínimos para os administradores e adicioná-las no grupo *wheel.*	9	TEC						
8	Permitir a elevação de privilégios através do comando su somente ao grupo *wheel.*	9	TEC						
9	Forçar o serviço SSH a aceitar conexões usando apenas a versão 2 do protocolo.	9	TEC						
10	Adicionar apenas as contas dos administradores no grupo *wheel.*	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
11	Desabilitar o acesso da conta *root* via SSH.	9	TEC						
12	Remover *banners* de identificação dos serviços habilitados.	9	TEC						
13	Habilitar o registro de acessos de usuários (arquivos *wtmp* e *btmp*).	9	TEC						
14	Habilitar *log* do sistema, separando por tipo de serviço.	9	TEC						
15	Habilitar o uso do PAM (*Pluggable Authentication Modules*).	9	TEC						
16	Habilitar o *flag* tcp_*syncookies* no TCP/IP para combater ataques do tipo *synflood.*	9	TEC						
17	Desabilitar a resposta a requisições ICMP em *broadcast* (ignore_*broadcasts*=1).	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
18	Desabilitar o aceite de pacotes IP roteados pela origem (*.accept_source_route= 0).	9	TEC						
19	Habilitar a verificação de caminho reverso para combater ataques de IP *spoofing* (*rp_filter=1).	9	TEC						
20	Adicionar as opções de montagem nosuid e noexec nas partições de dados (/home, /var etc).	9	TEC						
21	Adicionar as opções de montagem nosuid, noexec, nodev à partição /tmp.	9	TEC						
22	Adicionar as opções de montagem nodev, noexec e nosuid às mídias removíveis (fstab).	9	TEC						
23	Ajustar o tempo de ociosidade do console para 5 minutos.	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
24	O *layout* de particionamento do disco deve ser adequado (/boot, /, /home, /usr, /var, /tmp etc).	9	TEC						
25	Desabilitar desligamento do computador via CTRL+ALT+DEL.	9	TEC						
26	Remover o ambiente gráfico se ele não for estritamente necessário ao funcionamento de alguma aplicação.	9	TEC						
27	Habilitar o registro de eventos de uso do sistema (sysstat - comando sar).	9	TEC						
28	Habilitar o *sticky bit* nos diretórios públicos (/tmp por exemplo).	9	TEC						
29	Remover o suporte aos arquivos .rhosts do PAM.	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
30	Restringir o acesso ao agendador de tarefas (cron e at) apenas aos usuários autorizados.	9	TEC						
31	Definir e habilitar senha no gerenciador de inicialização (GRUB/Lilo) para restringir o acesso ao modo monousuário.	9	TEC						
32	Garantir que não haja nenhuma conta de usuário ativa com senha nula.	9	TEC						
33	Os diretórios dos usuários (/home) devem possuir atributos 0750 ou mais restritivos.	9	TEC						
34	Ajuste a máscara padrão de criação de arquivos e diretórios para 0770 (não acessíveis globalmente).	9	TEC						

Controles do sistema operacional Linux		*Tipo ame-aça*	*Tipo vuln.*	*Imple-men-tado*	*Custo estim. (HH)*	*Investi-mento estim. (R$)*	*Prob.*	*Im-pac-to*	*Risco*
#	*Controle*						*Nível*	*Nível*	*Nível*
35	Desabilitar a geração de core *dumps* quando programas são abortados.	9	TEC						
36	Desabilitar o *shell* de todas as contas de sistema (serviços).	9	TEC						

A.5 PLANO DE CONTINUIDADE DE NEGÓCIO: LISTAS

A.5.1 Lista de contatos para acionamento e os processos de negócios

A Tabela 193 (Lista de contatos para acionamento e os processos de negócios) apresenta a relação de contatos responsáveis para cada processo de negócio da empresa..

Tabela 193: Lista de contatos para acionamento e os processos de negócios

Nome	***Evento***	***Envolvi-mento***	***Tempo***	***Cargo***	***Área***	***Fone***	***e-mail***	***Substituto***
Nome1	Evento1	Envolvi-mento1	Tempo	Cargo1	Área1	Fone1	*e-mail1*	Substituto1
Nome2	Evento2	Envolvi-mento2	Tempo	Cargo2	Área2	Fone2	*e-mail2*	Substituto2
Nome3	Evento3	Envolvi-mento3	Tempo	Cargo3	Área3	Fone3	*e-mail3*	Substituto3
Nome4	Evento4	Envolvi-mento4	Tempo	Cargo4	Área4	Fone4	*e-mail4*	Substituto4
Nome5	Evento5	Envolvi-mento5	Tempo	Cargo5	Área5	Fone5	*e-mail5*	Substituto5

A.5.2 Lista de Fornecedores

A Tabela 194 (Lista de fornecedores) apresenta a relação fornecedores necessários caso o PCN seja acionado.

Tabela 194: Lista de fornecedores

Nome	*Endereço*	*Telefone*	*E- mail*	*Contato*	*Produto / Serviço*
Fornecedor1	Endereço1	Telefone1	*E-mail1*	Contato1	Produto/serviço1
Fornecedor2	Endereço2	Telefone2	*E-mail2*	Contato2	Produto/serviço2
Fornecedor3	Endereço3	Telefone3	*E-mail3*	Contato3	Produto/serviço3
Fornecedor4	Endereço4	Telefone4	*E-mail4*	Contato4	Produto/serviço4
Fornecedor5	Endereço5	Telefone5	*E-mail5*	Contato5	Produto/serviço5

A.5.3 Lista de Materiais

A Tabela 195 (Lista de Materiais) apresenta a relação de materiais necessários caso o PCN seja acionado.

Tabela 195: Lista de Materiais

Nome	*Descrição*	*Quantidade*
Material1	Descrição Material1	Quantidade1
Material2	Descrição Material2	Quantidade2
Materia3	Descrição Material3	Quantidade3
Material4	Descrição Material4	Quantidade4
Material5	Descrição Material5	Quantidade5

A.5.4 Lista de *Hardware* e *Software*

A Tabela 196 (Lista de *Hardware* e *Software*) apresenta a relação de *Hardware* e *Software* necessários caso o PCN seja acionado.

Tabela 196: Lista de *Hardware* e *Software*

Nome	***Quantidade***	***Fornecedor***
Nome1	Quantidade1	Fornecedor1
Nome2	Quantidade2	Fornecedor2
Nome3	Quantidade3	Fornecedor3
Nome4	Quantidade4	Fornecedor4
Nome5	Quantidade5	Fornecedor5