UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL**

ANDRÉ LUIZ SANTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

UMA PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA MELHORAMENTOS NORTE DO PARANÁ

Bandeirantes

2011

ANDRÉ LUIZ SANTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

UMA PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA MELHORAMENTOS NORTE DO PARANÁ

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, Campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Prof. Carlos Eduardo Ribeiro

Bandeirantes

2011

ANDRÉ LUIZ SANTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

UMA PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA MELHORAMENTOS NORTE DO PARANÁ

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, Campus Luiz Meneghel, como requisito parcial para a obtenção do grau de Bacharel em Sistemas de Informação.

COMISSÃO EXAMINADORA

_____

Prof. Carlos Eduardo Ribeiro
Campus Luiz Meneghel

_____

Prof. André Luis Andrade Menolli
Campus Luiz Meneghel

_____

Prof. José Reinaldo Merlin
Campus Luiz Meneghel

Bandeirantes, __ de_____ de 2011

DEDICATÓRIA

Dedico este trabalho aos meus pais, meu irmão e minha namorada por se fazerem presentes em minha vida a todo o momento e por me apoiarem em meus projetos e decisões, com estímulos que me impulsionaram a buscar vida nova a cada dia, concedendo a mim a oportunidade de me realizar e crescer ainda mais.

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me deu inteligência e capacidade de realizar meus planos, sendo que sem ele nada disso seria possível.

A minha família, pela ajuda, confiança, motivação e carinho.

A minha namorada, pelo amor, carinho e companheirismo que me motivam.

Ao Prof. Carlos Eduardo Ribeiro, o qual me orientou em todas as etapas deste trabalho.

Aos amigos e colegas de curso, pela determinação, companheirismo, força e coragem em relação a esta grande etapa de nossas vidas.

Aos professores, que de alguma forma contribuíram para o meu desenvolvimento no decorrer do curso.

A todos que, de alguma forma tiveram envolvimento e, com boa intenção, colaboraram para a realização e finalização deste trabalho.

"A vida é uma peça que não permite ensaios.

Por isso, cante, chore, dance, ria e viva intensamente,

Antes que a cortina se feche e a peça termine sem aplausos."

Charles Chaplin

RESUMO

Tudo que é importante para uma organização estruturada e de qualidade deve ser protegido, inclusive a informação, que é de grande valia como qualquer outro ativo dentro de uma empresa. Devido à importância da informação para o negócio nas organizações, faz-se necessário a definição e utilização de uma proteção apropriada que possa manter todas as informações distantes das diversas ameaças que possam vir a causar prejuízos à empresa e que possam também interferir na confidencialidade, integridade e disponibilidade das mesmas. A proteção das informações pode iniciar-se com a implantação de uma Política de Segurança da Informação, a qual estabelece procedimentos e regras que diminuem os riscos das informações sofrerem algum tipo de violação. O presente trabalho teve a intenção de contribuir no esclarecimento da maneira de se elaborar uma Política de Segurança padronizada, seguindo normas e padrões ISO, formulando uma Política de Segurança de acordo com a estrutura e objetivos de uma empresa do norte do Paraná. A política foi uma proposta implantada para com alguns usuários de alguns setores para a verificação de sua eficácia, que ficou aberta para possíveis modificações e melhorias.

Palavras-chave: Informação, Segurança da Informação, Política de Segurança.

ABSTRACT

All that is important to an organization structured and quality must be protected, including information that is valuable as any other asset within a company. Due to the importance of information for business organizations, it is necessary to the definition and use of proper protection that you can keep all the information away from various threats that may harm the company and may also interfere with the confidentiality, integrity and availability of same. The protection of information may begin with the establishment of an Information Security Policy, which establishes rules and procedures that reduce the risk of information suffer some sort of violation. This work was intended to contribute to clarify the way to develop a standardized Security Policy, following standards and ISO standards, formulating a security policy according to the structure and goals of a company in northern Paraná. The policy was implemented for a proposal with some users in some sectors to verify its effectiveness, which was open to possible modifications and improvements.

Keywords: Information, Information Security, Security Policy.

SUMÁRIO

1. INTRODUÇÃO

Juntamente com os avanços tecnológicos, a informação vem se tornando cada vez mais importante para as organizações, e devido a esta importância surge a necessidade de uma proteção adequada para a informação, a qual é um ativo essencial nos processos de tomada de decisão, na garantia da continuidade dos negócios, no aumento das oportunidades de negócios e em muitos outros parâmetros de negócio da empresa.

A informação nas organizações tem uma relação consideravelmente importante com os processos estratégicos, de negócios e produção, porém, o ativo de informação muitas vezes não recebe a devida proteção como os meios tangíveis e econômicos recebem. É importante que as organizações se prontifiquem a definir e utilizar uma proteção apropriada que mantenham as informações distantes das diversas ameaças que possam vir a causar um prejuízo à empresa e que possam interferir em três aspectos essenciais para as organizações em relação à informação, que são: Confidencialidade, Integridade e Disponibilidade.

Normalmente as organizações se preocupam com a segurança de suas informações a partir do momento que passam por algum incidente que gerou algum tipo de impacto aos seus negócios.

O presente trabalho abordou um estudo sobre Política de Segurança da Informação, enfatizando algumas práticas e metodologias para a elaboração de uma política eficaz, com a intenção de conscientizar e mostrar o quão é importante ter implantada uma Política de Segurança da Informação em uma organização. De acordo com conceitos obtidos em estudos bibliográficos, foram apresentados alguns métodos de criação de uma política de segurança para uma empresa.

No desenvolvimento deste trabalho, foi possível identificar alguns controles da norma NBR ISO/IEC 27002 que definiram uma Política de Segurança para as informações da Companhia Melhoramentos Norte do Paraná, empresa que serviu de base para o desenvolvimento e testes da política formulada.

1.1 METODOLOGIA DE PESQUISA

Para a realização deste trabalho foi utilizada a metodologia de pesquisa bibliográfica para o referencial teórico em artigos publicados na internet, livros e na norma NBR ISO/IEC 27002, tomando entendimento sobre a importância da Segurança da Informação e construindo uma visão de como se elaborar uma Política de Segurança da Informação.

Foi utilizada também a metodologia de estudo de caso pertinentes a maneira de manipulação da informação de uma organização do Paraná no ramo da produção de açúcar e álcool e liga de manganês. O estudo de caso serviu de suporte para a elaboração de uma proposta de Política de Segurança da Informação para a empresa, de acordo com seus objetivos e estratégias.

Com a intenção de melhorar a gestão da informação da organização, política elaborada poderá ser analisada, melhorada e implantada pela diretoria e equipe de TI da empresa.

1.2 JUSTIFICATIVA

A informação é um ativo de valor para as organizações que precisa ser protegida de alguma forma. Essa proteção pode ser feita de maneira apropriada através de uma Política de Segurança da Informação, a qual estabelece procedimentos e regras que diminuem os riscos de suas informações sofrerem algum tipo de violação ou perda que possam vir a ser prejudiciais aos objetivos da empresa.

A falta de proteção das informações pode causar perdas e danos irreparáveis aos negócios de uma empresa, por isso é necessário uma boa gestão de segurança das informações. O desenvolvimento do presente trabalho poderá contribuir e melhorar a visão das organizações e seus respectivos usuários sobre a importância da proteção da informação, e auxiliar nos possíveis desenvolvimentos de Políticas de Segurança da Informação.

1.3 OBJETIVOS

1.3.1 GERAL

O referido trabalho teve por objetivo geral, de acordo com a norma ISO/IEC 27002, identificar as melhores práticas de gestão da informação no quesito “Segurança”, contribuir e esclarecer a maneira de se elaborar uma Política de Segurança padronizada, formulando uma política para uma empresa do norte do Paraná, a Cia Melhoramentos, de acordo com a estrutura e objetivos da mesma, a fim de mostrar a esta empresa a importância de se ter implantada uma Política de Segurança da Informação.

1.3.2 ESPECÍFICOS

- Definir Política de Segurança e destacar suas características;
- Esclarecer a importância de se ter implantada uma Política de Segurança da Informação nas Organizações;
- Identificar os controles necessários para a política da organização; e
- Formular uma Política de Segurança da Informação para a empresa citada.

2 REFERENCIAL TEÓRICO

2.1 A IMPORTÂNCIA DAS INFORMAÇÕES

Informação é o elemento que sintetiza a natureza de qualquer entidade, expressando suas características (Caruso & Steffen, 1990).

Caruso & Steffen (1990) explicam que a informação pode ter seu valor avaliado de acordo com sua importância, utilidade e/ou valor financeiro para a organização.

A informação atualmente se tornou um recurso produtivo para as empresas e profissionais. Ela assume uma posição primordial e crescente nas corporações, pois define a importância e o valor de procedimentos, colaboradores (pessoas) e setores, além de ser um auxílio na geração de conhecimento e juntamente com os “dados”, a informação fornece suporte no processo de tomada de decisão das organizações.

Balloni (2002) argumenta que a informação é de valor altamente significativo e pode representar grande poder para quem a possui, seja pessoa, seja a organização.

A obtenção da informação é feita através do processamento dos dados existentes nas organizações, os quais são apenas registros brutos, que sozinhos, não têm muito valor. Chiavenato (2000) diz que os dados são elementos que servem de base para a formação de juízos ou para a resolução de problemas. Por isso, para se chegar à informação, os dados precisam passar por um processo de classificação, armazenamento e relacionamento, pois assim estarão ganhando significado e fornecendo informação.

Além de auxiliar no processo de tomada de decisão, a informação ajuda as organizações se manterem bem colocadas no mercado, contudo, ela precisa ser utilizada de forma eficaz, envolvendo o conhecimento de todos os membros das equipes, pois as informações contribuem com as previsões de oportunidades de investimento e tecnologias novas, e consequentemente, trazem destaque nas vantagens competitivas da empresa.

2.2 SEGURANÇA DA INFORMAÇÃO

A Tecnologia da Informação está cada vez mais alinhada com o planejamento estratégico das organizações, garantindo em muitos aspectos a competitividade das mesmas. De acordo com a norma ISO/IEC 27002 (2005), a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Proteger a informação pode gerar um árduo trabalho, devido à existência de várias formas de informação que necessitam ser protegidas. A implantação de metodologias de segurança da informação precisa ter o apoio constante da diretoria e dos gestores das organizações, pois estes estarão participando frequentemente das identificações de necessidades e da conscientização de usuários.

A norma ISO/IEC 27002 (2005), diz que:

> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversa. Seja qual for à forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida adequadamente.

Infelizmente não existe a possibilidade de comprar qualquer dispositivo que faça o papel de proteger a informação, pois a Segurança da Informação não é uma tecnologia.

Com base em Spanceski (2004) entende-se que segurança da informação é proteger a informação dos mais variados tipos de ameaça, como fraude, erros, sabotagens, perdas e outros, que possam inferir no fluxo dos negócios de uma organização.

A norma ISO/IEC 27002 (2005) diz que a Segurança da Informação é a preservação da confidencialidade, da integridade e da disponibilidade das informações, e também a garantia da autenticidade, responsabilidade, do não repúdio e confiabilidade das mesmas.

Essas características citadas acima envolvem alguns aspectos que as organizações precisam manter íntegros e atualizados, como sintetiza a Figura 01.

Figura 01: Aspectos da Garantia da Segurança (Fonte: Skylan Technology, 2010)

Treinamento: este envolve pessoas, as quais precisam estar treinadas, orientadas e conscientizadas dos objetivos da organização para com a segurança.

Processos: se refere ao controle e as regras para se utilizar os recursos tecnológicos e as informações da organização.

Tecnologia: aspecto que engloba a necessidade de se ter implantado sistemas que assegurem os objetivos da empresa.

A Skylan Technology, Consultoria e Suporte fornece um framework que modela o Sistema de Gestão de Segurança da Informação baseado na norma ISO/IEC 27002 (2005), mostrado na Figura 02.

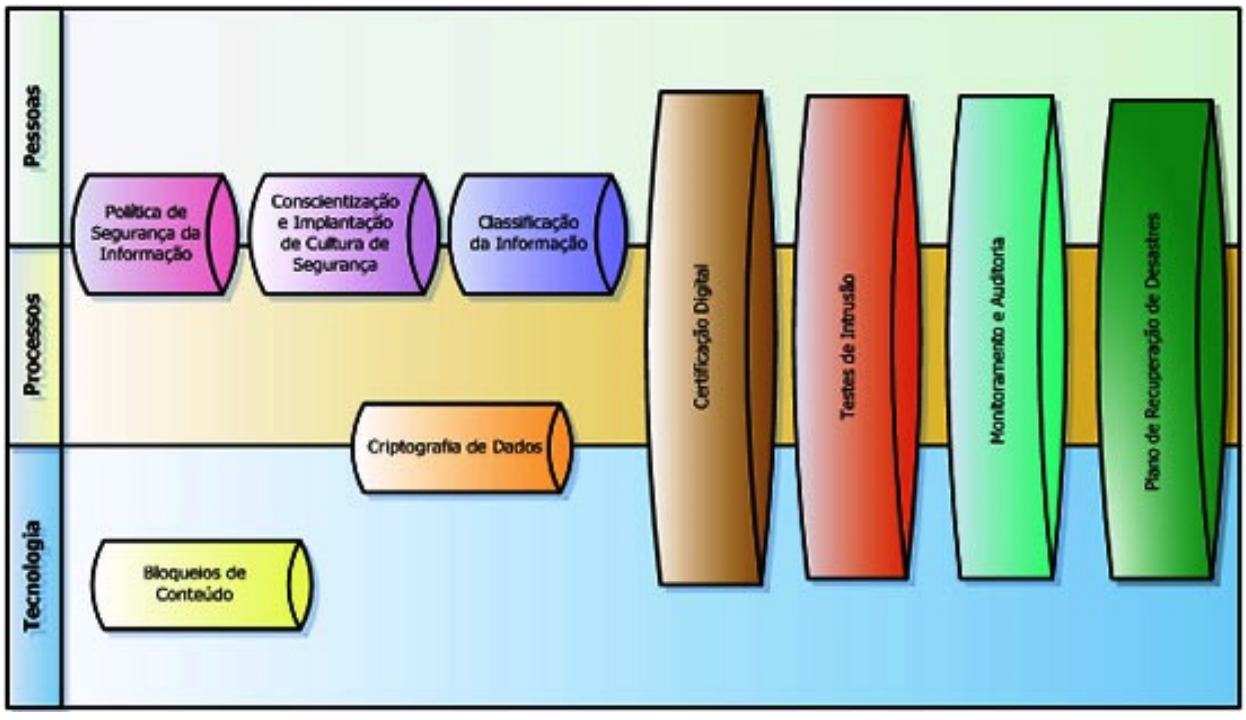


Figura 02: Framework do Sistema de Gestão da Segurança (Fonte: Skylan Technology, 2010)

Para alcançar a Segurança da Informação, é necessário controlar adequadamente as informações que precisam ser protegidas. A norma ISO/IEC 27002 (2005) mostra que esse controle adequado deve ser feito através de políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware, os quais devem ser acompanhados de forma crítica através de monitoramentos, análises e melhorias, quando necessário, pois só assim o objetivo da segurança da informação na organização será atingido.

As ameaças que colocam as informações e os sistemas de informação das organizações em risco são muitas, e devido a isto, se faz ainda mais necessário a busca pela segurança. Incêndio, inundação, fraudes eletrônicas, ataque de hackers, sabotagens e outros, são alguns exemplos dos tipos de ameaças existentes, os quais prejudicam de forma considerável o fluxo de negócio de uma organização.

Diminuir os riscos e a vulnerabilidade das informações às ameaças é um objetivo claro da Segurança da Informação, porém, o compartilhamento de recursos em redes públicas e privadas, e de uma forma mais ampla, a interconexão de redes, é algo que vem crescendo de forma rápida, e que infelizmente, dificulta o controle do acesso às informações, e conseqüentemente, a segurança fica menos eficaz. Por isso, a participação e comprometimento de todos os membros da organização fazem-se necessária para o sucesso da Segurança da Informação.

Spanceski (2004) diz que o processo de segurança começa e termina nas pessoas, e que a eficiência das políticas e dos procedimentos desse processo se dá no comprometimento das pessoas para com o uso desses mecanismos de segurança e da consciência dos mesmos de que o benefício para o organização será excepcionalmente positivo.

2.3 NÍVEIS DE SEGURANÇA DA INFORMAÇÃO

A informação, para ser protegida, precisa receber um determinado nível de segurança, que se baseie no valor daquela informação e da necessidade de mesma para a organização. A informação precisa ser classificada.

De acordo com a norma ISO/IEC 27002 (2005):

> A classificação da informação tem o objetivo de assegurar que a informação receba um nível adequado de proteção. Ela precisa ser classificada para

> indicar a necessidade, prioridades e o nível esperado de proteção. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial.

A definição e classificação dos níveis de segurança de cada informação presente em um determinado setor é uma atividade que deve ser realizada pelo proprietário da informação e/ou o responsável por aquele setor, pois é ele quem melhor conhece as informações ali presentes.

O item 7.1.2 da norma ISO/IEC 27002 (2005) esclarece que todas as informações e ativos associados com os recursos de processamento da informação necessitam de um proprietário designado por uma parte definida da organização, e mais:

> O proprietário do ativo é responsável por assegurar que as informações estejam adequadamente classificadas e ainda precisa definir e periodicamente analisar as classificações e restrições ao acesso, levando em conta as políticas de controle de acesso.

A informação pode ser classificada com o objetivo de atender duas necessidades, sendo a necessidade de proteção contra revelação e a necessidade de preservação da informação. Caruso e Steffen (1999) mostram um modelo de classificação da informação para cada necessidade citadas acima.

Na necessidade de proteção contra revelação, a informação pode ser classificada como: secreta, confidencial e uso interno (CARUSO & STEFFEN, 1999).

2.3.1 Secreta

Este tipo de informação é de extrema importância para a organização e que indiscutivelmente, deve ter sua integridade preservada. Por isso, devem ser acessadas por um número restrito de pessoas sendo totalmente controladas sobre o uso de tais informações. O acesso interno ou externo por pessoas não autorizadas a esse tipo de informação é extremamente crítico para a empresa. São informações vitais para a organização (SPANCESKI, 2004).

2.3.2 Confidencial

São informações que se forem acessadas de forma não autorizada, podem trazer danos irreparáveis para a Organização, como danos no ambiente financeiro da empresa, brechas para a concorrência e conseqüentemente, perda da confiança dos clientes.

Devido a esses danos, esse tipo de informação deve ficar restrita ao ambiente da empresa, onde as mesmas só devem ser acessadas perante uma necessidade que seja fundamental para o desenvolvimento de uma determinada tarefa de um ou mais usuários que possam acessá-las (SPANCESKI, 2004).

2.3.3 Interna

Informações internas são aquelas que devem ficar disponíveis apenas para a organização, sendo que o acesso externo destas deve ser evitado. Estas informações, se por acaso, vazarem do âmbito da empresa, não trarão nenhum dano crítico para a mesma, porém, podem causar algum prejuízo de forma indireta para a organização e denegrir de forma mínima a imagem desta.

2.4 OBJETIVOS E PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Fornecer a informação certa, na hora certa e para a pessoa certa é algo essencial para uma tomada de decisão rápida e eficaz. Isto traz um grande diferencial para as organizações, fazendo-as destacar-se perante a concorrência, além da satisfação dos usuários em ter informações confiáveis e corretas no momento que precisam.

A Segurança da Informação das organizações precisa conquistar a plena confiança e satisfação dos usuários, pois estes esperam que as informações só sejam acessadas por aqueles que podem acessá-las, e para conquistar essa confiança e satisfação e ainda atender várias outras expectativas dos usuários, é preciso que a segurança da informação tenha quatro objetivos e/ou princípios em relação aos ativos protegidos, que são: Autenticidade e Não Repúdio, Disponibilidade, Confidencialidade e Integridade (SPANCESKI, 2004).

2.4.1 Autenticidade e Não Repúdio

O objetivo da autenticidade é garantir que a informação é procedente da fonte informada em seu conteúdo. Este controle garante e verifica a identidade e autenticidade de uma pessoa ou sistema que transmite uma mensagem e/ou informação, mantendo íntegra a origem do ativo.

De acordo com Spanceski (2004):

> O controle de autenticidade está com a identificação de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos.

2.4.2 Disponibilidade

A disponibilidade consiste em assegurar o acesso à determinada informação por um usuário autorizado. É prover um acesso seguro e confiável e que esteja prontamente disponível a quem necessita.

Exemplo: se um usuário fizer uma alteração em qualquer informação que ele não tenha autorização e no mesmo momento o usuário proprietário daquela informação tentar acessá-la, esta deve estar disponível para o proprietário sem qualquer alteração que não tenha sido feita por ele (SPANCESKI, 2004).

Uma informação ou um sistema não disponível no momento necessário poder causar o mesmo impacto de uma informação excluída ou de um sistema inexistente.

2.4.3 Confidencialidade

Manter uma informação confidente é evitar que ela seja acessada por um usuário que não tenha permissão do proprietário em qualquer tipo de acesso na mesma (leitura, cópia, edição, exclusão, etc.).

Spanceski (2004) relata que o objetivo da confidencialidade é proteger a informação privada de agentes internos e/ou externos.

Exemplo: um usuário do Departamento Fiscal de uma organização não poderá ter acesso às informações de cargos e salários da mesma organização, pois esta é uma informação que deve estar disponível apenas para a diretoria e para o Departamento de Recursos Humanos.

2.4.4 Integridade

De acordo com Araújo (2008) a integridade é garantir que a informação manipulada mantenha as características originais, que foram estabelecidas pelo proprietário daquela informação. Garantindo a integridade, será possível evitar que dados de uma determinada informação sejam apagados ou alterados sem o consentimento do proprietário.

No controle da integridade o conceito de “dados” é um pouco mais amplo. Baseando em Spanceski (2004), dados podem ser considerados programas, documentação, fitas magnéticas, registros, etc. o autor ainda diz que:

> A integridade de dados também é um pré-requisito para outros princípios e objetivos da segurança. Por exemplo, se a integridade de um sistema de controle a um determinado sistema operacional pode ser violada, então a confidencialidade de seus arquivos pode ser igualmente violada.

Por isso, faz-se muito importante a preservação da integridade dos dados e informações das organizações, juntamente com todos os outros princípios e objetivos da segurança da informação.

De acordo com Silva (2004) a Autenticidade e Não Repúdio, a Disponibilidade, a Confidencialidade e a Integridade são os pilares da Segurança da Informação, ou seja, são características essenciais para a proteção dos ativos desejados, como é mostrado na Figura 03.

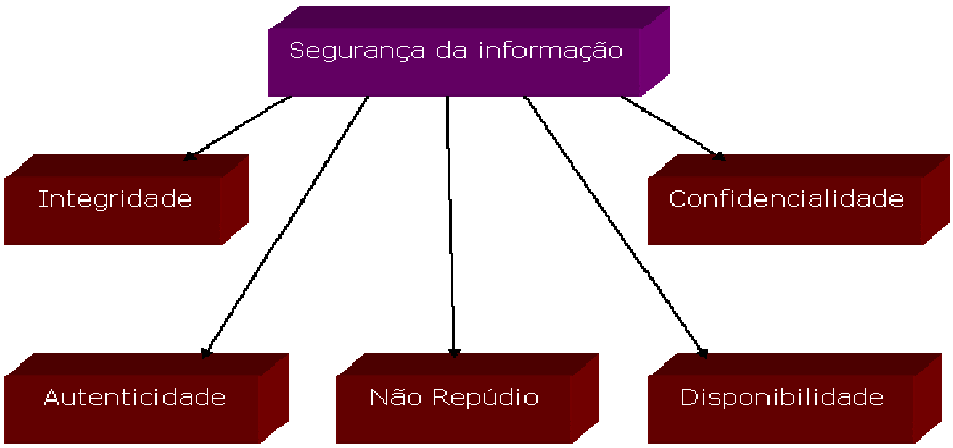


Figura 03: Pilares da Segurança da Informação (Fonte: SILVA, Antonio Mendes da, 2004)

2.5 POLÍTICA DE SEGURANÇA

Uma Política de Segurança é a definição de normas e procedimentos, ferramentas e responsabilidades, que visam minimizar os riscos dos ativos de uma organização, como por exemplo, a informação, ou seja, é a definição de melhores práticas para a manipulação das informações.

De acordo com Spanceski (2004), a Política de Segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribuem e limitam direitos e responsabilidades às pessoas que trabalham com a informação, e também impõe penalidades quanto ao descumprimento da Política.

A norma NBR ISO/IEC 27002 (2005) mostra que o documento de Política deve conter:

- Uma definição de segurança da informação, suas metas globais e princípios da segurança da informação, de acordo com os objetivos da organização;
- Uma declaração do comprometimento da direção, apoiando as metas e princípios da segurança da informação;
- Uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de risco;
- Relação de princípios, normas e requisitos de conformidade de segurança, específicos para a organização;

- Uma definição das responsabilidades gerais e específicas na gestão da segurança da informação, incluindo o registro de incidentes;
- Referências a documentação que possam apoiar a política, como regras de segurança que os usuários devem seguir.

Uma Política de Segurança bem elaborada poderá trazer muitos benefícios para a organização, pois esta esclarecerá o que será protegido, de quem será protegido e por que será protegido, minimizando assim, os danos ou ocorrências que podem afetar as informações da organização.

Porém, não basta somente ter uma Política de Segurança implantada, é preciso ter apoio e responsabilidades por parte da direção e dos usuários da organização para seguir essa Política. Com base em Spanceski (2004), é preciso assegurar que a utilização da política seja eficaz e efetivamente utilizada, e uma forma de realizar esse processo, de "controle do uso da política" é através de auditorias permanentes, as quais verificam a existência de uma política e ainda, se as normas e procedimentos estão sendo seguidos.

2.5.1 Níveis da Política de Segurança

Nem todas as políticas envolvem todos os controles de uma norma ou todas as leis existentes relacionadas ao assunto, sendo assim, uma política pode ser dividida em níveis diferentes.

Segundo Dimitri (2002, citado por Spanceski, 2004), uma política de segurança pode ser dividida em três níveis: estratégico, tático e operacional.

O nível estratégico se refere a uma política ou parte dela onde as normas, ferramentas e/ou procedimentos são definidos com base no bom senso dos profissionais, seguindo os valores da empresa.

O nível tático refere-se a uma política que visa à padronização das definições, fazendo com que todos os pontos da empresa trabalhem com o mesmo nível de segurança, com equipamentos, senhas e outros no mesmo padrão de utilização.

O nível operacional é a parte mais detalhada da política, onde se encontra o detalhamento de todas as configurações do ambiente, de forma padronizada, ou seja, se aplica da mesma forma para todos os pontos da organização.

2.5.2 Tipos de Política

Spanceski (2004) expõe três tipos distintos de políticas de segurança: Regulatória, Consultiva e Informativa.

A Regulatória é uma política bem detalhada, com especificações legais e geralmente direcionada para um ramo específico de atividade.

A Consultiva é uma política que oferece métodos e ações para a realização das atividades de uma organização. Esta não é obrigatória, mas sua utilização é recomendada juntamente com a conscientização dos usuários, pois muitos riscos podem ser evitados com a aplicação de uma política consultiva.

A Informativa é uma política sem detalhamento de métodos ou ações, e a não utilização de mesma não oferecerá riscos a organização, porém esta pode trazer informações relevantes como a informação da aplicação de penalidades para com os usuários em atitudes que contradizem o rumo da organização.

2.6 NORMA NBR ISO/IEC 27002

A ISO/IEC 27002 é uma versão internacional do BS 7799, que se refere a um padrão internacional voltado aos controles de segurança da informação. Foi adotada pela ISO (*International Organization for Standardization*) e pelo IEC (*International Engineering Consortium*) em dezembro de 2000, sofrendo algumas alterações nos anos seguintes.

Em agosto de 2001, o Brasil adotou esta norma como padrão, por meio da ABNT (Associação Brasileira de Normas Técnicas), denominando-a NBR ISO/IEC 17799, a qual começou a ser modificada em 2005 e em 2007 passou a ser incorporada com a nova numeração NBR ISO/IEC 27002.

A norma tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação nas organizações.

O “Código de Prática para a Gestão de Segurança da Informação” possui 11 seções de controles, sendo:

- Política de Segurança da Informação;
- Organizando a Segurança da Informação;

- Gestão de Ativos;
- Segurança em Recursos Humanos;
- Segurança Física e do Ambiente;
- Gestão das Operações e Comunicações;
- Controle de Acesso;
- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;
- Gestão de Incidentes de Segurança da Informação;
- Gestão da Continuidade do Negócio;
- Conformidade.

Não há a necessidade de aplicação de todos os controles de todas as seções nos processos das organizações. O grau de importância de cada seção deve ser definido de acordo com a necessidade de cada organização, tanto que a norma não prioriza e nem distingue uma seção da outra se baseando na importância de cada uma.

Esta norma foca em três premissas principais da Segurança da Informação, que são confidencialidade, integridade e disponibilidade, as quais já foram definidas anteriormente.

3 DESENVOLVIMENTO

O desenvolvimento do presente trabalho teve o objetivo de trazer como resultado uma Política de Segurança da Informação voltada para os objetivos da Companhia Melhoramentos Norte do Paraná.

A política criada foi de caráter regulatório, com nível tático, com definições baseadas na norma ISO/IEC 27002 e também baseadas nos objetivos da empresa, ou seja, normas específicas da companhia.

3.1 A COMPANHIA MELHORAMENTOS NORTE DO PARANÁ

A Companhia Melhoramentos Norte do Paraná, formada por três filiais, atua nas áreas de produção de Açúcar, Álcool Etílico Hidratado e Anidro Carburantes na Companhia Agrícola Usina Jacarezinho, unidade de Jacarezinho, no estado do Paraná, na produção de Álcool Etílico Hidratado e Anidro Carburantes na Destilaria Melhoramentos, unidade de Jussara, Paraná, e também produz também liga de Manganês Alto Carbono e Liga de Silício Manganês na Maringá S/A Cimento e Ferro-Liga, na unidade de Itapeva, estado de São Paulo.

No quesito qualidade, a empresa procura atingir os seguintes objetivos:

- Ser um fornecedor confiável de produtos com qualidade, conforme requisitos especificados pelo cliente/mercado;
- Alcançar produtividade e custos necessários para manter a competitividade da empresa;
- Prover a segurança e proteger a saúde dos colaboradores e de todos aqueles que intervêm nos locais de trabalho; e
- Buscar a melhoria contínua da eficácia do Sistema de Gestão da Qualidade e respeitar o meio-ambiente.

A área de Tecnologia da Informação da organização procura trabalhar com alguns padrões definidos pela própria área, só que nem todos os usuários têm o conhecimento de tais padrões.

A empresa possui um servidor específico para os acessos à internet, outro para acesso a email, um terceiro para acesso interno (pastas e documentos da empresa) e um último, que se refere a um servidor de backup e contingência.

Quando contratados, os usuários recebem um login e uma senha para fazerem os acessos aos micros, emails e sistemas internos (ERP's, Help Desk, etc.), cada um com um acesso diferenciado, de acordo com a necessidade.

As caixas de emails possuem uma limitação de tamanho específica, de acordo com a utilização de cada usuário. O acesso à internet é limitado a alguns usuários, e os que têm tal acesso, são impossibilitados de fazerem downloads.

Os acessos a pastas e arquivos são liberados de acordo com o setor do usuário, por exemplo: se um usuário faz parte do departamento da Contabilidade, ele tem acesso a todos os arquivos daquele setor, o que nem sempre é necessário e conveniente.

A empresa possui vários procedimentos que contribuem para uma melhora na Gestão de Informação da mesma, porém, as normas e procedimentos ali existentes não estão totalmente documentados e nem esclarecidos a todos os usuários.

De acordo com a TI da organização, a falta de tempo e dedicação foram um tipo de empecilho para o desenvolvimento de uma política para empresa, mas o reconhecimento da necessidade de um documento que contribua para a melhoria da gestão da informação está presente na área.

3.2 UMA POLÍTICA PARA COMPANHIA MELHORAMENTOS NORTE DO PARANÁ

A Política de Segurança que o presente trabalho propõe para a Companhia Melhoramentos Norte do Paraná (CMNP), disponível no apêndice A deste trabalho, trata dos aspectos básicos da área de informação da empresa, focando a proteção dos dados e processos importantes da mesma, definindo um padrão de segurança a ser seguido pela gerência e usuários comuns, internos e externos, com maior foco no risco humano.

A definição da Política seguiu o seguinte caminho:

1. Conceituação da Política de Segurança e seus objetivos;
2. Definições para a classificação das informações;
3. Definições para Usuário e Senha de Acesso à Rede;
4. Definições de Direito de Acesso às Informações;
5. Definições para a Utilização dos Recursos de TI;
6. Definições para Instalação e uso de Softwares;
7. Definições para Admissão, Demissão e Transferência de Funcionários;
8. Definições para o uso de Internet;
9. Definições para o uso de Correio Eletrônico (email);
10. Definições para o uso de Antivírus;
11. Definições para cópias de segurança (backup); e
12. Definições para acessos a áreas e recursos físicos.

3.2.1 Definindo os Controles

Como já foi citada anteriormente, a norma NBR ISO/IEC 27002 possui 11 seções com diversos controles, porém, não existe a obrigação da utilização de todos os controles existentes.

Abaixo estão relacionados os controles da norma NBR ISO/IEC 27002 utilizados para o desenvolvimento da política da CMNP.

Na seção 5 – "Política de Segurança da Informação":

- Categoria 5.1 – "Política de segurança da informação"

1. Controle *“5.1.1 – Documento da Política de Segurança da Informação”*;

Na seção 6 – “Organizando a Segurança da Informação”:

- Categoria 6.1 – “Organização interna”
    2. Controle 6.1.2 – *“Coordenação da Segurança da Informação”*;
    3. Controle 6.1.3 – *“Atribuição de responsabilidades para a Segurança da Informação”*;
    4. Controle 6.1.4 – *“Processo de autorização para os recursos de processamento da Informação”*;
    5. Controle 6.1.5 – *“Acordos de confidencialidade”*;

- Categoria 6.2 – “Partes Externas”
    6. Controle 6.2.1 – *“Identificação dos riscos relacionados com partes externas”*;
    7. Controle 6.2.3 – *“Identificando segurança da informação nos acordos com terceiros”*;

Na seção 7 – “Gestão de Ativos”:

- Categoria 7.1 – “Responsabilidade pelos ativos”
    8. Controle 7.1.1 – *“Inventário dos Ativos”*;
    9. Controle 7.1.2 – *“Proprietário dos Ativos”;*
    10. Controle 7.1.3 – *“Uso aceitável dos Ativos”;*

- Categoria 7.2 – “Classificação da informação”
    11. Controle 7.2.1 – *“Recomendações para classificação”;*

Na seção 8 – “Segurança em recursos humanos”:

- Categoria 8.1 – “Antes da contratação”
    12. Controle 8.1.1 – *“Papéis e responsabilidades”;*
    13. Controle 8.1.3 – *“Termos e condições de contratação”;*

- Categoria 8.2 – “Durante a contratação”
    14. Controle 8.2.1 – *“Responsabilidades da direção”;*
    15. Controle 8.2.2 – *“Conscientização, educação e treinamento em segurança da informação”;*
    16. Controle 8.2.3 – *“Processo disciplinar”;*

- Categoria 8.3 – “Encerramento ou mudança da contratação”
    17. Controle 8.3.3 – *“Retirada de direitos de acesso”;*

Na seção 9 – “Segurança física e do ambiente”:

- Categoria 9.1 – “Áreas Seguras”
    18. Controle 9.1.1 – “Perímetro de segurança física”;
    19. Controle 9.1.2 – “Controles de entrada física”;

- Categoria 9.2 – “Segurança de equipamentos”
    20. Controle 9.2.2 – “Utilidades”;
    21. Controle 9.2.3 – “Segurança do Cabeamento”;

Na seção 10 – “Gerenciamento das operações e comunicações”:

- Categoria 10.4 – “Proteção contra códigos maliciosos e códigos móveis”
    22. Controle 10.4.1 – “Controles contra códigos maliciosos”;

- Categoria 10.5 – “Cópias de segurança”
    23. Controle 10.5.1 – “Cópias de segurança das informações”;

- Categoria 10.7 – “Manuseio de mídias”
    24. Controle 10.7.1 – “Gerenciamento de mídias removíveis”;
    25. Controle 10.7.2 – “Descarte de mídias”;

- Categoria 10.10 – “Monitoramento”
    26. Controle 10.10.1 – “Registros de auditoria”;
    27. Controle 10.10.2 – “Monitoramento do uso do sistema”;

Na seção 11 – "Controle de acessos":

- Categoria 11.1 – "Requisitos de negócio para controle de acesso"
  28. Controle 11.1.1 – "Política de controle de acesso";

- Categoria 11.2 – "Gerenciamento de acesso do usuário"
  29. Controle 11.2.1 – "Registro de usuário";
  30. Controle 11.2.2 – "Gerenciamento de privilégios";
  31. Controle 11.2.3 – "Gerenciamento de senha do usuário";
  32. Controle 11.2.4 – "Análise crítica dos direitos de acesso de usuário";

- Categoria 11.3 – "Responsabilidades dos usuários"
  33. Controle 11.3.1 – "Uso de senhas";
  34. Controle 11.3.3 – "Política de mesa limpa e tela limpa";

- Categoria 11.4 – "Controle de acesso à rede"
  35. Controle 11.4.1 – "Política de uso dos serviços de rede";

Na seção 13 – "Gestão de incidentes de segurança da informação":

- Categoria 13.1 – "Notificação de fragilidade e eventos de segurança da informação"
  36. Controle 13.1.2 – "Notificando fragilidades de segurança da informação";

Na seção 15 – "Conformidade":

- Categoria 15.1 – "Conformidade com requisitos legais"
  37. Controle 15.1.4 – "Proteção de dados e privacidade de informações pessoais";
  38. Controle 15.1.5 – "Prevenção de mau uso de recursos de processamento da informação";

- Categoria 15.2 – “Conformidade com normas e políticas de segurança da informação e conformidade técnica”

39. Controle 15.2.1 – “Conformidade com as políticas e normas de segurança da informação”;

Apesar dos controles citados servirem de base para o desenvolvimento da política de segurança, a maioria das normas e procedimentos existentes nela foram elaborados de acordo com as metodologias de trabalho da empresa CMNP.

4 RESULTADOS

A política de segurança da informação formulada foi implantada em três setores de uma das unidades da CMNP, a unidade de Jacarezinho, Paraná.

Os setores da Companhia Agrícola Usina Jacarezinho que “testaram” a política foram:

- Recursos Humanos;
- Contabilidade;
- Desenvolvimento Agrícola.

Inicialmente a política foi aplicada para três colaboradores de cada um dos setores citados, para que se pudesse verificar a diferença na execução das atividades com o uso de uma política de segurança e sem o uso da mesma. A aplicação se deu com algumas restrições e modificações nos acessos dos usuários e treinamento dos mesmos nas diretrizes da política.

Os setores escolhidos possuíam uma duplicidade muito grande de documentos, conhecimento de senhas do usuário vizinho para executar algumas atividades, acessos a arquivos e pastas desnecessários e um alto tráfego de emails.

A aplicação da política se deu por um período de 31 dias (maio de 2011) nos setores citados, e para verificar a diferença e/ou resultado, foi verificado o número de chamados abertos para o Help Desk da TI pelos usuários da política antes da aplicação e durante a aplicação das normas e procedimentos, e também foi aplicado um questionário aos usuários antes e depois da política, de modo que eles pudessem expressar as diferenças que perceberam com a utilização de uma política de segurança.

A área de TI da CMNP é dividida em quatro subáreas, onde cada área atua com um ou dois colaboradores nas unidades da CMNP, com um supervisor para cada área, sendo:

1. *Gestão Empresarial:* responsável pelos ERP’s utilizados na empresa;
2. *Banco de Dados:* área responsável pela manutenção do banco de dados dos servidores ERP’s da empresa;
3. *Infra-estrutura e hardware:* área de TI responsável pela disponibilidade dos hardwares (equipamentos físicos).

4. *Redes e Aplicativos:* responsável pela integridade e disponibilidade dos sistemas operacionais dos servidores e das estações de trabalho, dos backups, dos arquivos e pastas da rede e dos acessos dos usuários de rede.

Em relação aos chamados, foi observada uma diferença de 20% a menos no número de chamados abertos pelos usuários dos setores utilizadores da política.

Nas Figuras 04, 05 e 06 são mostrados os relatórios de estatísticas do Sistema de Gerenciamento da Informática, Help Desk da TI da CMNP:

Relatório do Período de aplicação da Política de Segurança

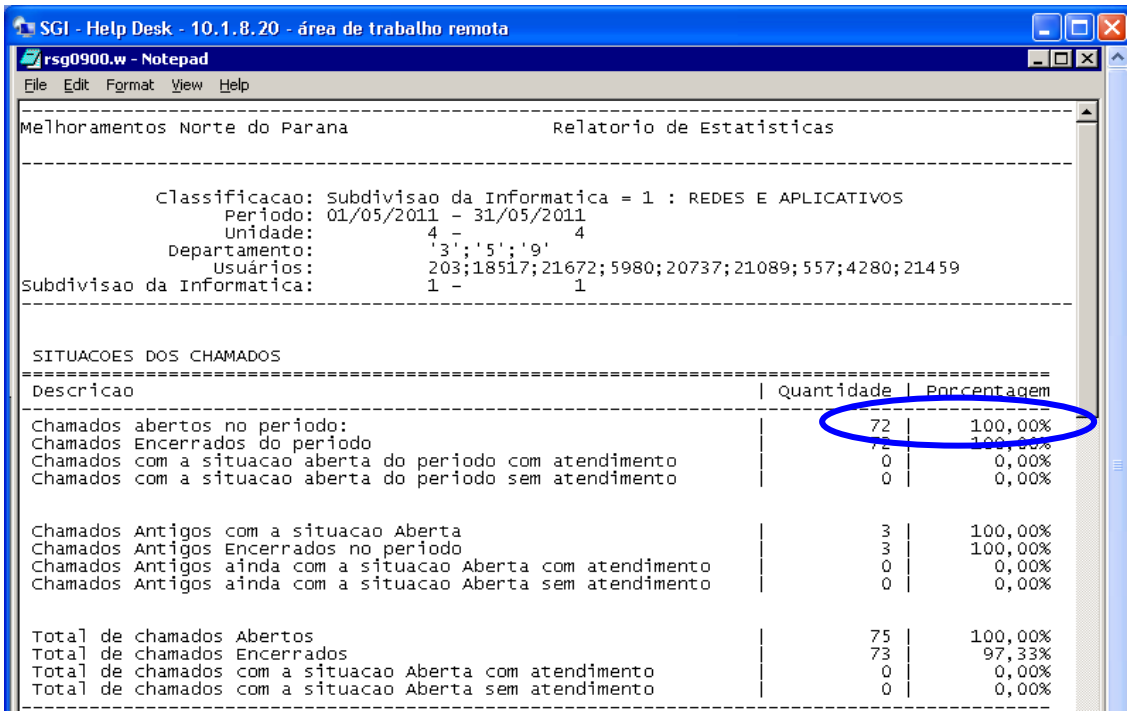
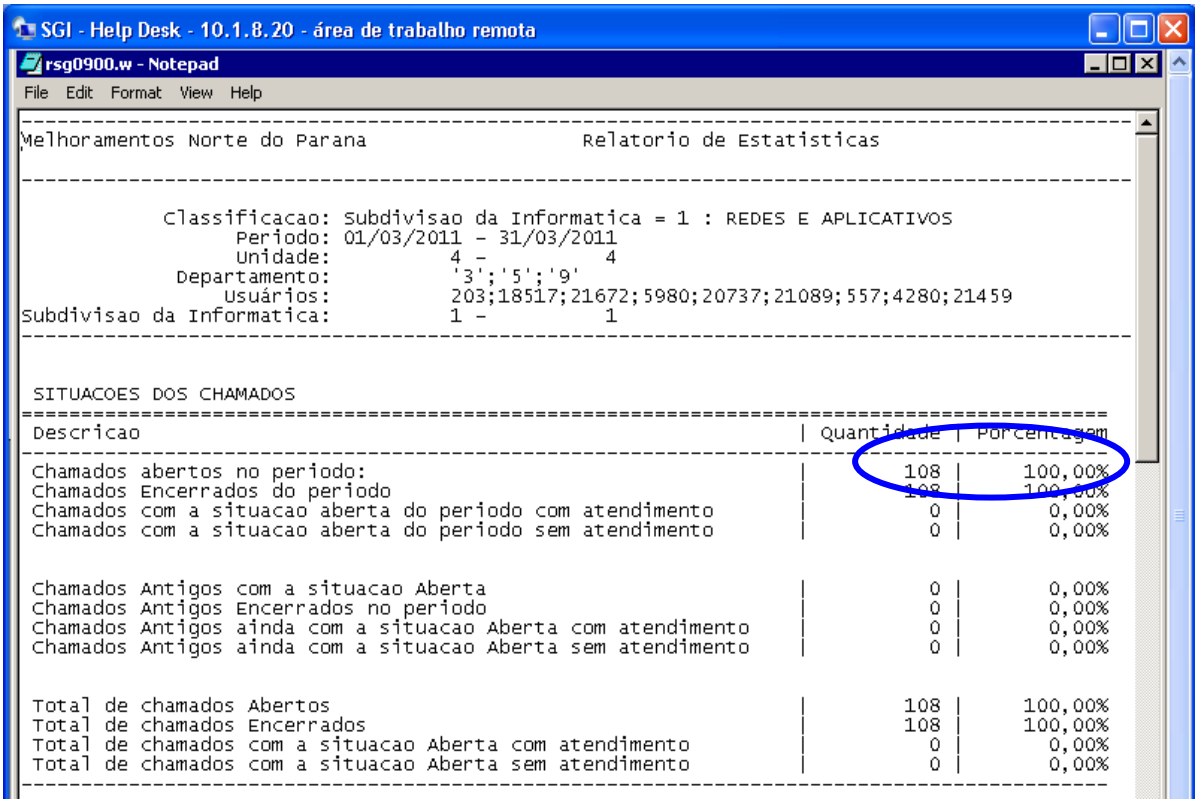


Figura 04: Relatório de Chamados Abertos no período de 01/05/2011 à 31/05/2011 (Fonte: Sistema de Gerenciamento da Informática da CMNP, 2011)



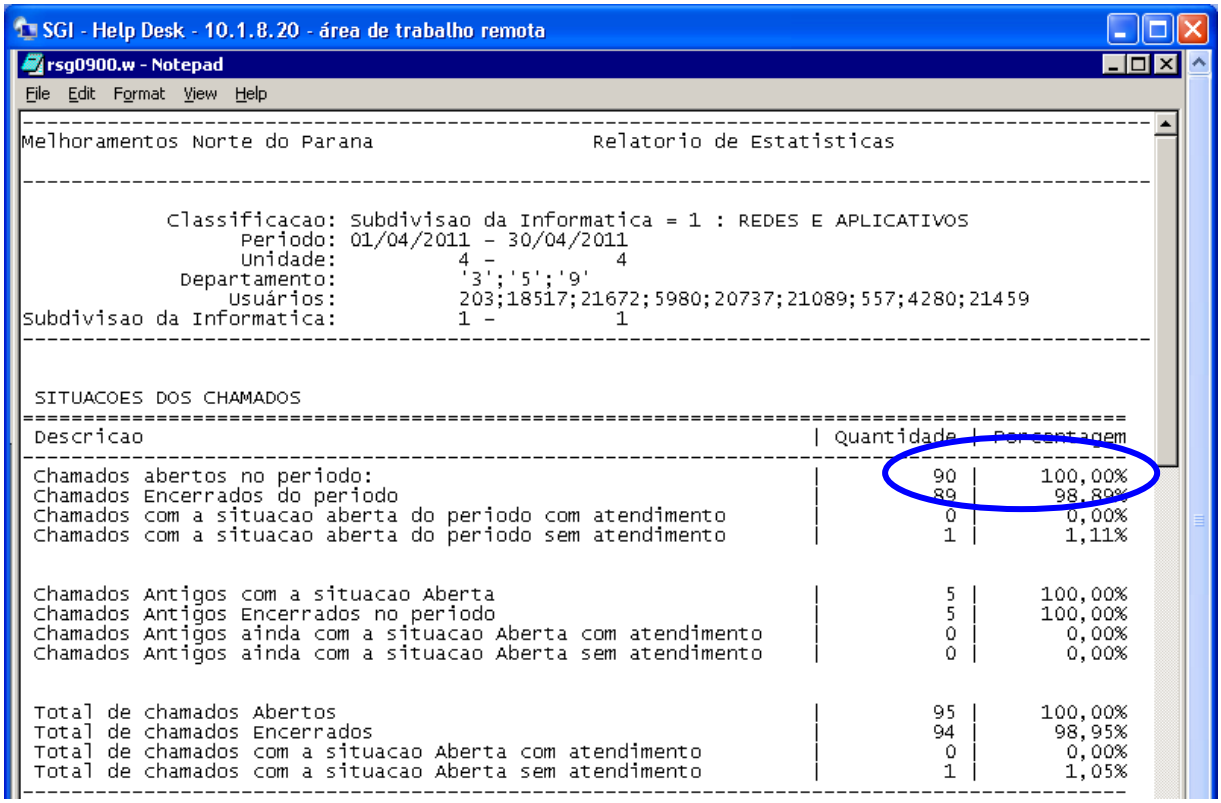
SGI - Help Desk - 10.1.8.20 - área de trabalho remota

rsg0900.w - Notepad

File Edit Format View Help

```
Melhoramentos Norte do Parana                  Relatorio de Estatisticas

            Classificacao: Subdivisao da Informatica = 1 : REDES E APLICATIVOS
                  Periodo: 01/03/2011 - 31/03/2011
                  Unidade:          4 -           4
             Departamento:          '3';'5';'9'
                 Usuários:          203;18517;21672;5980;20737;21089;557;4280;21459
Subdivisao da Informatica:          1 -           1


 SITUACOES DOS CHAMADOS
 Descricao                                                          | Quantidade | Porcentagem
 Chamados abertos no periodo:                                       |        108 |     100,00%
 Chamados Encerrados do periodo                                     |        108 |     100,00%
 Chamados com a situacao aberta do periodo com atendimento          |          0 |       0,00%
 Chamados com a situacao aberta do periodo sem atendimento          |          0 |       0,00%

 Chamados Antigos com a situacao Aberta                             |          0 |       0,00%
 Chamados Antigos Encerrados no periodo                             |          0 |       0,00%
 Chamados Antigos ainda com a situacao Aberta com atendimento       |          0 |       0,00%
 Chamados Antigos ainda com a situacao Aberta sem atendimento       |          0 |       0,00%

 Total de chamados Abertos                                          |        108 |     100,00%
 Total de chamados Encerrados                                       |        108 |     100,00%
 Total de chamados com a situacao Aberta com atendimento            |          0 |       0,00%
 Total de chamados com a situacao Aberta sem atendimento            |          0 |       0,00%
```

Figura 05: Relatório de Chamados Abertos no período de 01/03/2011 à 31/03/2011 (Fonte: Sistema de Gerenciamento da Informática da CMNP, 2011)



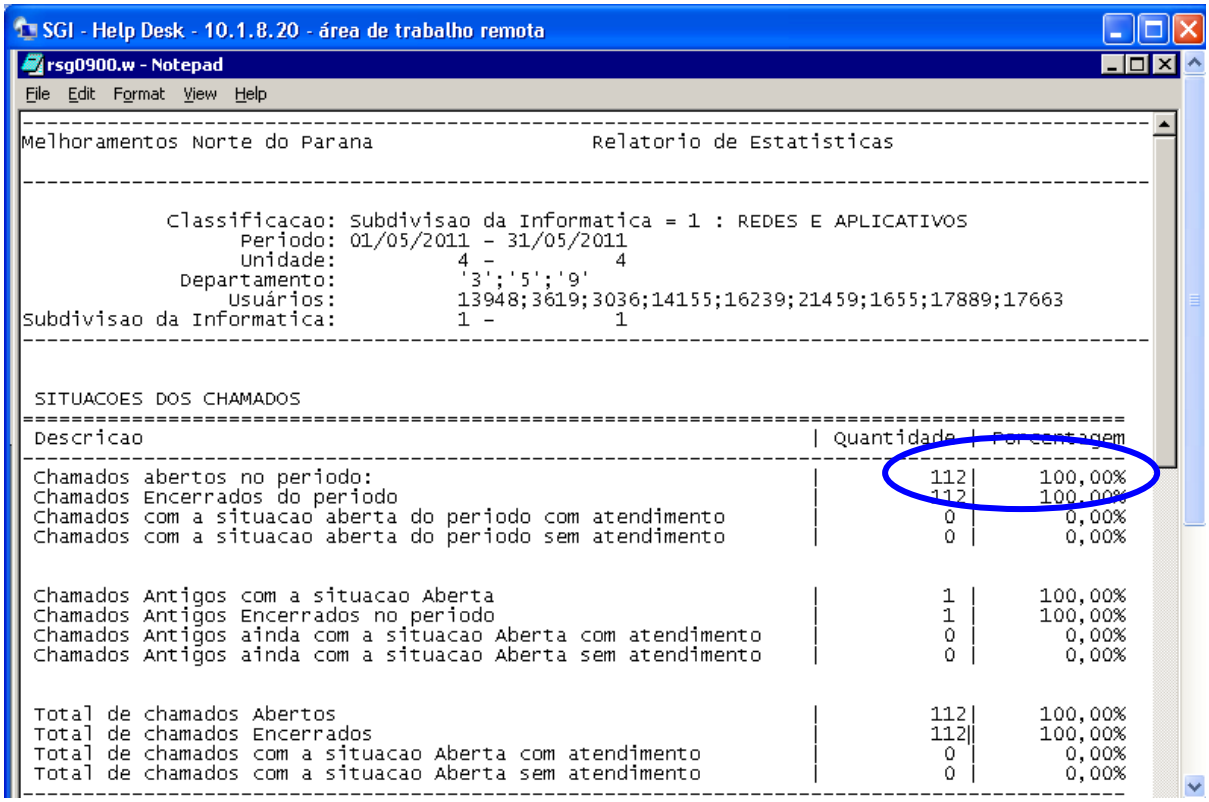
SGI - Help Desk - 10.1.8.20 - área de trabalho remota

rsg0900.w - Notepad

File Edit Format View Help

```
Melhoramentos Norte do Parana                  Relatorio de Estatisticas

            Classificacao: Subdivisao da Informatica = 1 : REDES E APLICATIVOS
                  Periodo: 01/04/2011 - 30/04/2011
                  Unidade:          4 -           4
             Departamento:          '3';'5';'9'
                 Usuários:          203;18517;21672;5980;20737;21089;557;4280;21459
Subdivisao da Informatica:          1 -           1


 SITUACOES DOS CHAMADOS
 Descricao                                                          | Quantidade | Porcentagem
 Chamados abertos no periodo:                                       |         90 |     100,00%
 Chamados Encerrados do periodo                                     |         89 |      98,89%
 Chamados com a situacao aberta do periodo com atendimento          |          0 |       0,00%
 Chamados com a situacao aberta do periodo sem atendimento          |          1 |       1,11%

 Chamados Antigos com a situacao Aberta                             |          5 |     100,00%
 Chamados Antigos Encerrados no periodo                             |          5 |     100,00%
 Chamados Antigos ainda com a situacao Aberta com atendimento       |          0 |       0,00%
 Chamados Antigos ainda com a situacao Aberta sem atendimento       |          0 |       0,00%

 Total de chamados Abertos                                          |         95 |     100,00%
 Total de chamados Encerrados                                       |         94 |      98,95%
 Total de chamados com a situacao Aberta com atendimento            |          0 |       0,00%
 Total de chamados com a situacao Aberta sem atendimento            |          1 |       1,05%
```

Figura 06: Relatório de Chamados Abertos no período de 01/04/2011 à 30/04/2011 (Fonte: Sistema de Gerenciamento da Informática da CMNP, 2011)



SGI - Help Desk - 10.1.8.20 - área de trabalho remota

rsg0900.w - Notepad

File Edit Format View Help

Melhoramentos Norte do Parana — Relatorio de Estatisticas

Classificacao: Subdivisao da Informatica = 1 : REDES E APLICATIVOS
Periodo: 01/05/2011 - 31/05/2011
Unidade: 4 - 4
Departamento: '3';'5';'9'
Usuários: 13948;3619;3036;14155;16239;21459;1655;17889;17663
Subdivisao da Informatica: 1 - 1

SITUACOES DOS CHAMADOS

Descricao	Quantidade	Porcentagem
Chamados abertos no periodo:	112	100,00%
Chamados Encerrados do periodo	112	100,00%
Chamados com a situacao aberta do periodo com atendimento	0	0,00%
Chamados com a situacao aberta do periodo sem atendimento	0	0,00%
Chamados Antigos com a situacao Aberta	1	100,00%
Chamados Antigos Encerrados no periodo	1	100,00%
Chamados Antigos ainda com a situacao Aberta com atendimento	0	0,00%
Chamados Antigos ainda com a situacao Aberta sem atendimento	0	0,00%
Total de chamados Abertos	112	100,00%
Total de chamados Encerrados	112	100,00%
Total de chamados com a situacao Aberta com atendimento	0	0,00%
Total de chamados com a situacao Aberta sem atendimento	0	0,00%

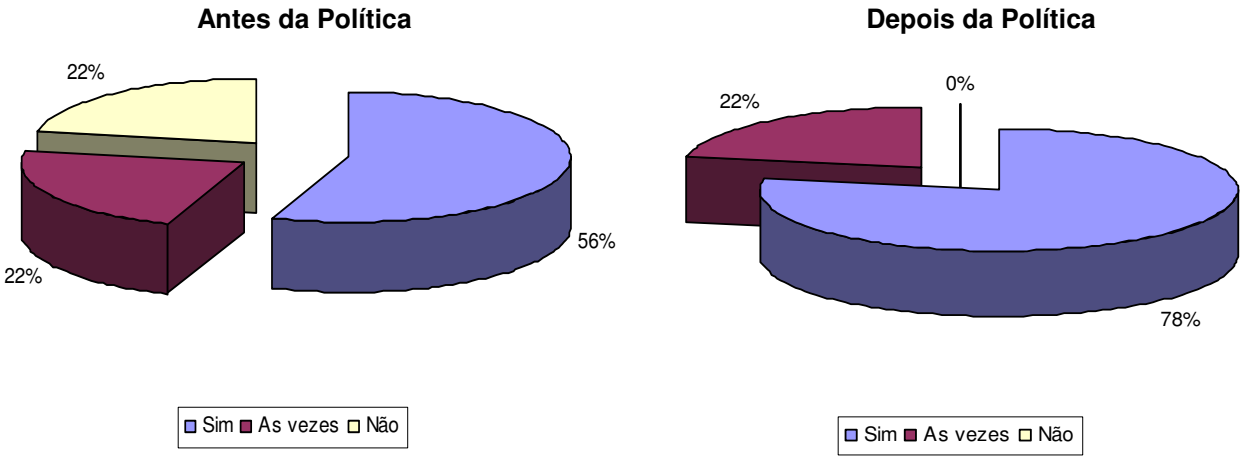
Figura 06: Relatório de Chamados Abertos no período de 01/05/2011 à 31/05/2011 por outros usuários com as mesmas funções dos mesmos setores (Fonte: Sistema de Gerenciamento da Informática da CMNP, 2011)

Essa comparação do número de chamados foi realizada apenas com os chamados relacionados à área de Redes e Aplicativos, que está mais ligada às normas e procedimentos da política. São chamados relacionados a travamento de senhas de login, acesso a pastas, recuperação de arquivos, instalação de programas e outros.

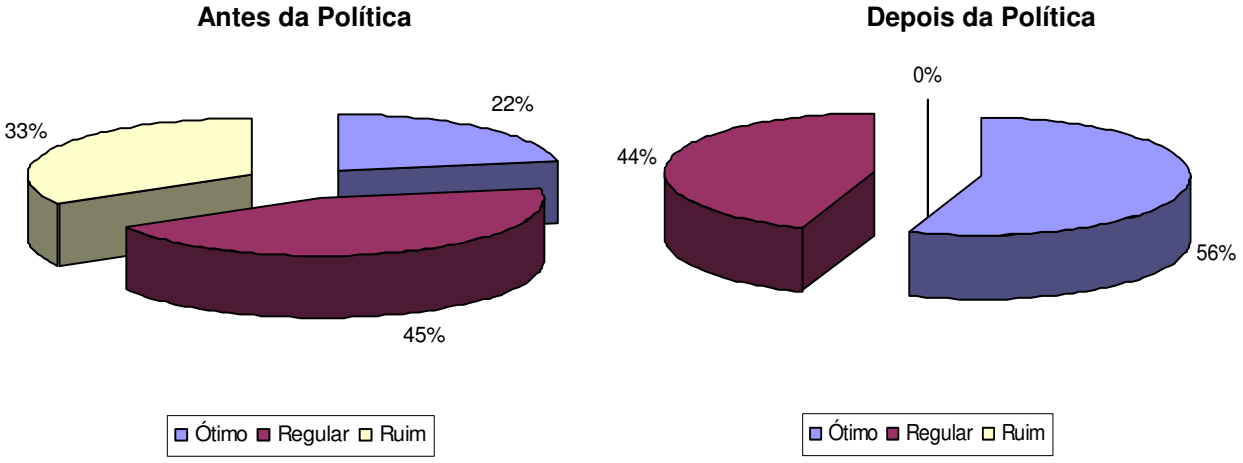
4.1 APLICAÇÃO DO QUESTIONÁRIO

Para contribuir com a verificação do resultado, foi aplicado um questionário aos 9 usuários da política de segurança, o qual o modelo se encontra no apêndice B deste trabalho e apresentou o seguinte resultado:

1 - As informações que necessitam estão sempre disponíveis?

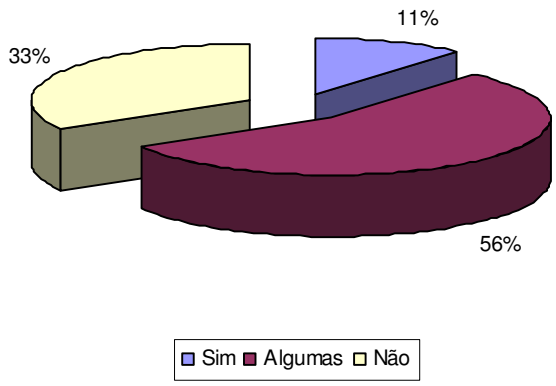


2 – Como avaliaria a segurança das informações que você trabalha?

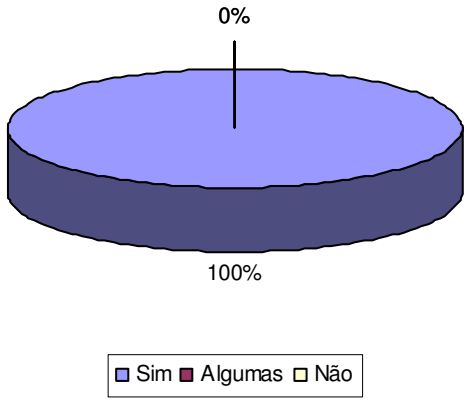


3 – Você tem conhecimento de suas limitações de acesso à internet?

Antes da Política

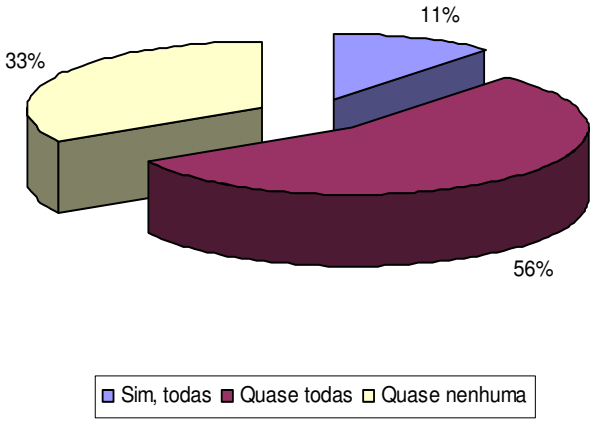


Depois da Política

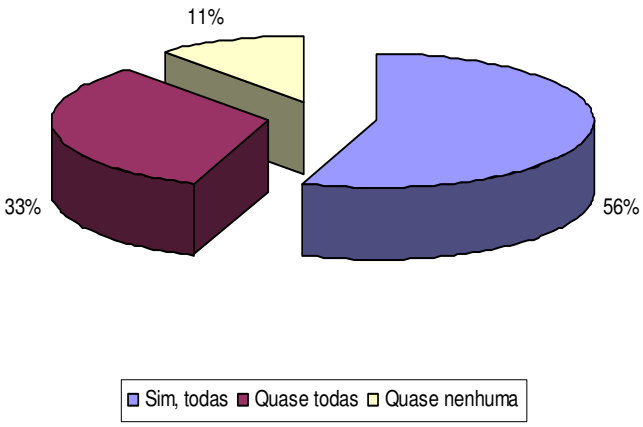


4 – Você necessita e utiliza todas as pastas que têm acesso?

Antes da Política

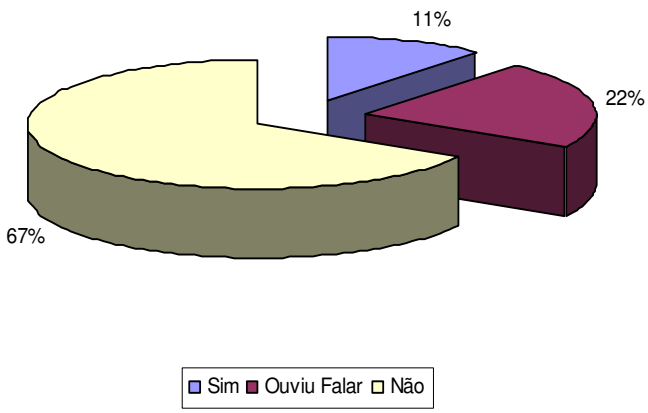


Depois da Política

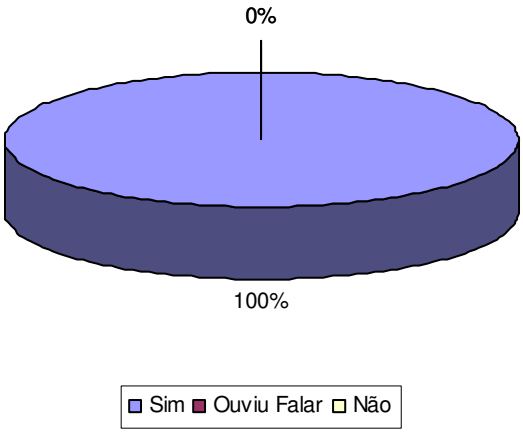


5 – Conhece documentos formalizando as restrições da área de TI?

Antes da Política

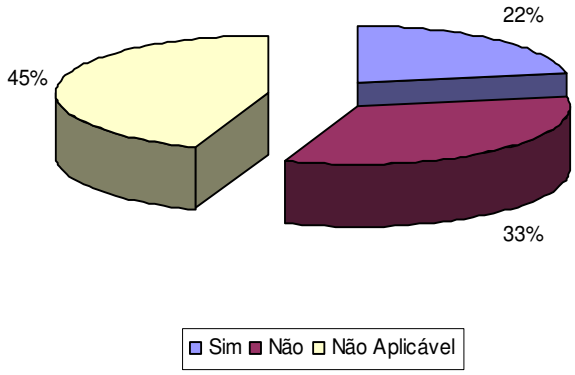


Depois da Política

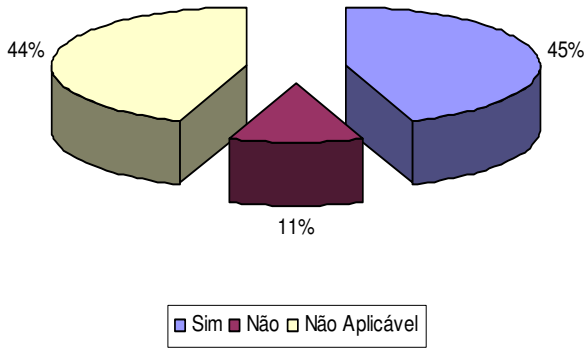


6 – Os arquivos utilizados em conjunto estão sempre íntegros e atualizados?

Antes da Política

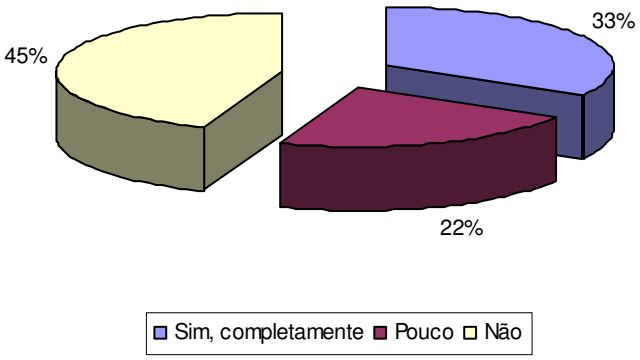


Depois da Política

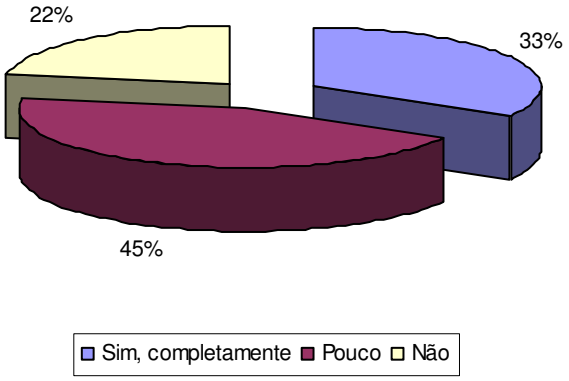


7 – Seu gestor está envolvido com suas necessidades de utilização da informação?

Antes da Política

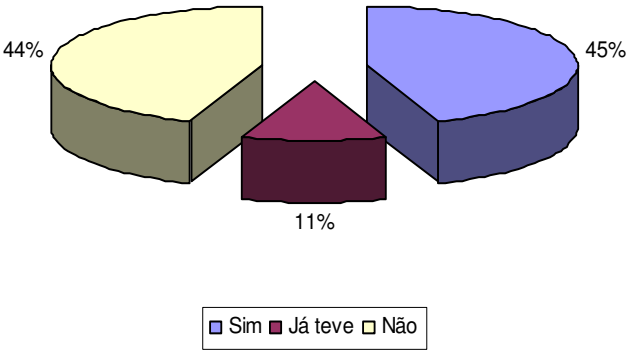


Depois da Política

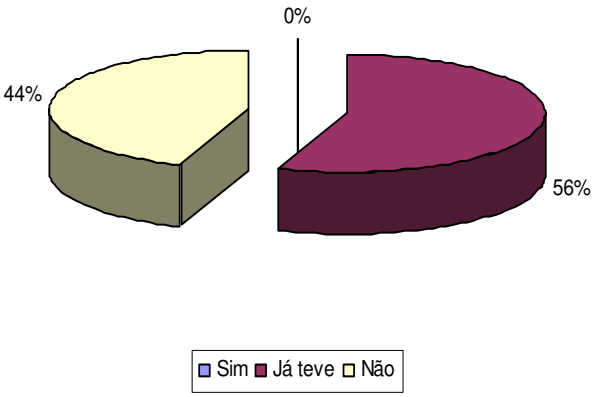


8 – Uma segunda pessoa tem conhecimento de sua senha de email ou de login?

Antes da Política

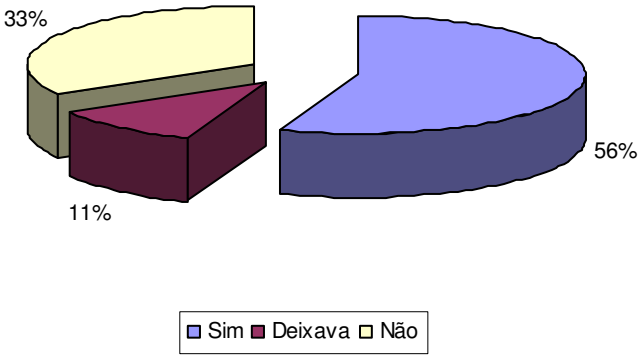


Depois da Política

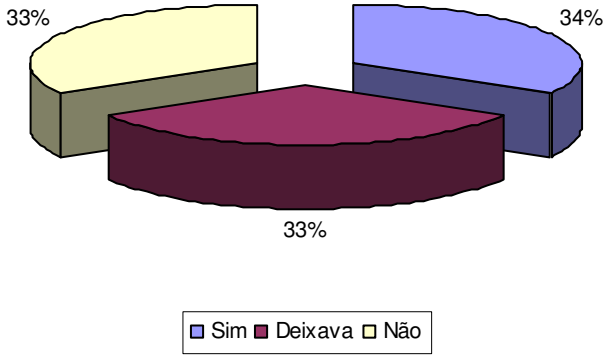


9 – Deixa documentos e/ou relatórios sobre mesas, impressoras ou abertos em tela?

Antes da Política

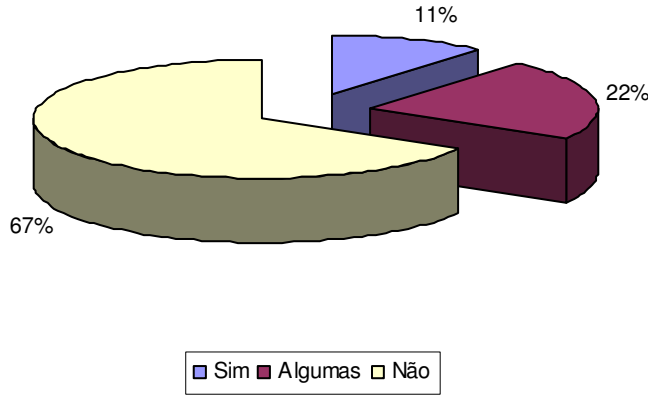


Depois da Política

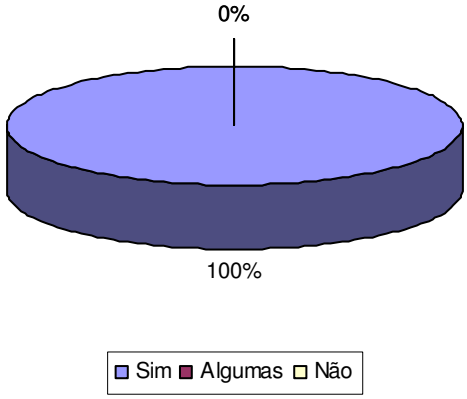


10 – Conhece as penalidades que podem ser aplicadas pelo mau uso da informação?

Antes da Política



Depois da Política



Com o resultado obtido através do questionário foi possível perceber que existem várias situações que ocorrem pela falta de conhecimento dos usuários para com suas limitações.

Existem casos que usuários cometem negligência por pura e espontânea vontade em comunhão com sua falta de ética profissional, mas se existirem normas, diretrizes, regras e procedimentos disponíveis ao entendimento de todos os usuários, o número de incidentes e negligências cometidos por risco humano será menor.

Dos nove colaboradores da CMNP entrevistados, quase 70% deles não tinham conhecimento de qualquer tipo de penalidade que pode ser aplicada por motivos de mau uso da informação, e quase todos tinham acesso a pastas que eram

desnecessárias para a realização de suas atividades, e as encaminhadas à TI nem sempre eram de conhecimento de seus gestores.

É fato que vários problemas podem ser resolvidos com a implantação de uma política de segurança da informação, como por exemplo, a diminuição da duplicação de arquivos nos servidores e, consequentemente menor gasto com hardwares, o conhecimento por parte dos gestores nos acessos de seus subordinados, o aumento na confidencialidade das informações disponíveis, pastas e arquivos mais íntegros sendo que estes passam a ser acessados somente pelos seus verdadeiros proprietários e maior agilidade na execução das atividades devido à melhor organização da informação da empresa.

5 CONSIDERAÇÕES FINAIS

As informações vêm tomando cada vez mais espaço no nível de importância dos ativos das organizações, com isso é indispensável que elas tenham uma proteção apropriada que as distanciem das mais diversas ameaças e vulnerabilidades, evitando o comprometimento da confiabilidade, da integridade e da disponibilidade dessas informações.

Uma política de segurança é a ferramenta mais eficaz para tratar da proteção das informações, pois é nela que estão definidos os procedimentos, normas, ferramentas e responsabilidades para a manipulação da informação pelos usuários.

Este trabalho abordou os conceitos de segurança da informação, juntamente com seus objetivos e princípios, a importância das informações, os níveis de segurança da informação, parte do histórico e conceitos da norma NBR ISO/IEC 27002 e os conceitos e desenvolvimento de uma política de segurança, sendo este último o principal objetivo do trabalho.

A política desenvolvida teve como foco os objetivos e a estrutura organizacional da empresa Companhia Melhoramentos Norte do Paraná (CMNP) e base nos procedimentos da norma NBR ISO/IEC 27002, a qual possui diversos controles que, se atendidos, garantem que a empresa tenha uma boa gestão da segurança de suas informações.

A política formulada em um nível tático, padroniza regras para todos os ambientes da organização possibilitando a garantia de todos usuários seguirem tais regras da mesma maneira, fazendo com que as negligências e incidentes cometidos por falta de conhecimento das regras pelos usuários sejam menores.

Uma política de segurança da informação é um diferencial bastante importante para as organizações, e assim, a política desenvolvida juntamente com o estudo realizado deixa algumas contribuições, sendo:

- Melhor entendimento sobre segurança da informação e sua importância;
- Melhor entendimento da função e do controles da norma NBR ISO/IEC 27002;
- A identificação da necessidade de mudanças no comportamento e participação dos usuários da informação; e

- Formulação de uma política de segurança da informação.

O trabalho fica aberto para projetos futuros, onde muitas outras regras ainda podem ser inclusas na política, tratando, por exemplo:

- Análise e avaliação de riscos;
- Segurança física e do ambiente da informação;
- Auditoria dos sistemas de informação;
- Análise e modelagem de um Plano de Continuidade do Negócio relativo à segurança da informação; e outros.

Inicialmente, a Política foi uma proposta apresentada a organização que se necessário, ainda poderá passar por modificações e melhorias para ser implantada na empresa, com a necessidade da participação de todos os gestores, para que todos os usuários fiquem cientes de suas limitações e acessos, e conseqüentemente, melhor orientados sobre a forma de trabalharem com as informações ali presentes.

REFERÊNCIAS

ARAÚJO, Nonata Silva. **Segurança da Informação**. O Portal da Administração. Julho de 2008. Disponível em: http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acessado em: 14 de outubro de 2010.

BALLONI, Antonio José. **Porque gestão em sistemas e tecnologias da informação?** Revista Unicamp, Campinas, 2002. Disponível em: http://www.ccuec.unicamp.br/revista/infotec/artigos/balloni.html>. Acessado em: 13 de outubro de 2010.

CARDOSO, Fernando Henrique. **Lei 9.609 – Programas de Computador**. Fevereiro de 1998. Disponível em: http://www.planalto.gov.br/ccivil/Leis/L9609.htm. Acessado em: 17 de outubro de 2010.

CARUSO, Carlos A. A., STEFFEN, Flávio Deny. **Segurança em Informática e de Informações**. Editora SENAC: São Paulo, 1999.

CHIAVENATO, Idalberto. **Introdução à teoria geral da administração**. 6. ed. rev. e atual. Rio de Janeiro: Campus, 2000.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação.** 1. ed.. Rio de Janeiro: Axcel, 2000.

FARIA, Alexia Lage. **Segurança da Informação: uma visão focada nos negócios.** Disponível em: http://www.profissionaisti.com.br/2010/02/seguranca-da-informacao-uma-visao-focada-nos-negocios/. Acessado em 15 de fevereiro de 2011.

FARIA, Alexia Lage. **Conheça a NBR ISO/IEC 27002 – Parte 1.** Disponível em: http://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-1/. Acessado em 17 de fevereiro de 2011.

FARIA, Alexia Lage. **Conheça a NBR ISO/IEC 27002 – Parte 2.** Disponível em: http://www.profissionaisti.com.br/2010/03/conheca-a-nbr-isoiec-27002-parte-2/. Acessado em 17 de fevereiro de 2011.

LAUDON, Kenneth C., LAUDON, Jane Price. **Sistemas de Informações Gerenciais.** Person Prentice Hall: São Paulo, 2004.

LAUREANO, Marcos Aurélio Pchek. **A Importância da Informação**. PUC, PR. Fevereiro de 2008. Disponível em: http://www.ppgia.pucpr.br/~euclidesfjr/SEGURANCA_DA_INFORMACAO/gst_cap_02_2008.pdf. Acessado em: 14 de outubro de 2010.

LONGO, Gustavo Dobkowski. **Segurança da Informação**. Universidade Estadual Paulista. Faculdade de Ciências Campus de Bauru. Disponível em: <http://www.firewalls.com.br/files/ArtigoCientifico.pdf. Acessado em: 02 de agosto de 2010.

MAGALHÃES, J. A. P. **Gestão do Conhecimento**. Dissertação de Mestrado. PUC-RIO, 2002.

NBR ISO/IEC 27002:2005. **Tecnologia da Informação – Código de Prática para Gestão da segurança de Informações**. 2ª ed.Rio de Janeiro, 2005.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia de informação aplicada a sistemas de informação empresariais.** São Paulo: Atlas, 2001.

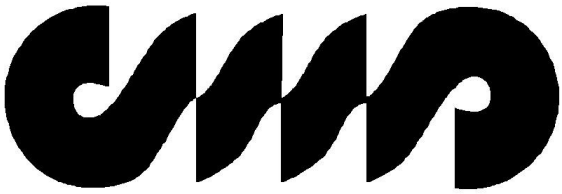
SILVA, Antonio Mendes Filho. **Segurança da Informação: Sobre a Necessidade de Proteção de Sistemas de Informações**. Revista Espaço Acadêmico Nº42, 2004.

SKYLAN TECHNOLOGY – Consultoria e Suporte. **Segurança da Informação.** Disponível em: http://www.skylan.com.br/?pg=pagina&id=23. Acessado em 22 de outubro de 2010.

SPANCESKI, Francini Reitz. **Política de Segurança da Informação: Desenvolvimento de um modelo voltado para instituições de ensino**. Instituto Superior Tupy – Joinville. Dezembro de 2004.

APÊNDICES

Apêndice A – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DA CMNP



Política de Segurança da Informação

Companhia Melhoramentos Norte do Paraná

ÍNDICE

1. Definição

Política de Segurança é a definição de normas e procedimentos, ferramentas e responsabilidades, que visam minimizar os riscos e proteger as informações da organização das mais variadas ameaças internas e/ou externas, físicas e/ou humanas.

A ausência de uma política de segurança da informação pode oferecer alguns riscos à empresa e aos usuários da informação da mesma.

As regras, aqui estabelecidas visam doutrinar e orientar o comportamento ético e profissional de nossos colaboradores ou contratados, no que se refere à utilização dos ativos, prevendo ações de segurança, para reduzir riscos, garantir a proteção dos dados da empresa, seus fornecedores e clientes. Também servir de referência para auditoria, apuração e avaliação de responsabilidades.

Arquivos diversos, emails, internet, mídias, documentos impressos e banco de dados são vistos pela organização como sendo um ativo para a organização. Sendo assim, os procedimentos e normas presentes, terão o objetivo de manter a confidencialidade, a integridade e a disponibilidade dos ativos da CMNP.

1.1 Risco à empresa

- Roubo de dados;
- Divulgação indevida de dados a concorrentes, fornecedores, clientes, terceiros;
- Desvios de ética, abusando do serviço para fins pessoais, comerciais, acadêmicos e até mesmo de espionagem, fornecendo informações confidenciais a concorrentes;
- Invasão do sistema por terceiros, já que este recurso se utiliza da Internet para enviar e receber informações a partir da residência ou qualquer outro local externo à organização pelo detentor da funcionalidade

1.2 Riscos ao usuário

- Perda de trabalho realizado;

- Transtornos à sua área, áreas concomitantes ou à organização como um todo;
- Punições previstas pela legislação vigente;
- No caso de demissão por justa causa, más referências a um suposto novo emprego;
- Roubo de informações confidenciais, seja de caráter pessoal, acadêmico ou profissional

2. Objetivo

A política de segurança da informação da CMNP visa garantir a autenticidade, disponibilidade, integridade e a confidencialidade de todas as informações necessárias para o negócio da empresa, definindo e formalizando normas e procedimentos que assegurem direitos e responsabilidades aos funcionários, fornecedores e clientes, mantendo:

- A proteção dos registros organizacionais;
- A correta utilização das informações;
- A proteção de dados e privacidade de informações departamentais e pessoais;
- A atribuição de responsabilidades aos colaboradores para com a segurança da informação;
- A conscientização e orientação no comportamento ético profissional de todos que utilizam recursos computacionais.

3. Responsáveis

Convém que as atividades de segurança da informação sejam coordenadas por representantes de diferentes partes da organização, com funções e papéis relevantes (NBR ISO/IEC 27002, item 6.1.2).

Os gestores da informação deverão garantir a execução das atividades de segurança da informação, conduzir as não-conformidades conforme necessário e identificar ameaças para a informação.

Os colaboradores responsáveis pela aplicação da presente política são os colaboradores da área de TI, sendo: Supervisora Geral de informática, Supervisores de Informática, Analistas de Suporte e Analistas de Sistema.

4. Documentação Associada

PSQ "Administração de Banco de Dados e Sistema de Gestão", PSQ "Implantação e Utilização de Software de Gestão (ERP/ADM/INDL/AGRIC)" e PSQ "Administração de Infra-Estrutura, Hardware, Rede e Software".

5. Condições Necessárias

- Microcomputador.
- Acesso à rede.
- Acesso ao Sistema de Gerenciamento da Informática (SGI).
- Acesso a email interno e/ou externo via GroupWise.

6. Abrangência

A presente política aplica-se a todos os colaboradores, clientes e terceiros que tenham acesso e utilizam os recursos de tecnologia da informação da empresa. Todos estes tem a obrigação de seguir as normas e procedimentos desta política.

7. Cuidados com Pessoal e Equipamentos

– Durante o trabalho manter sempre uma boa postura (evite posturas torcidas e assimétricas): entre braço/antebraço e coxa/perna manter um ângulo de aproximadamente 90º. A inclinação do encosto da cadeira deve ficar entre 90º a 110º. A cabeça deve ficar com inclinação neutra, nem inclinada muito para trás ou para frente. O mouse deve ficar no mesmo nível do teclado.

– Monitor do computador: manter-se distante aproximadamente, ao equivalente o cumprimento dos braços do usuário. A altura do monitor deve ter sua metade superior na mesma altura de seus olhos. Não deve posicionar de frente para janelas ou outra fonte luminosa intensa.

– Procure variar de postura, se estiver muito tempo sentado procure levantar-se e alongar-se. Recomendam-se pausas de alguns minutos a cada hora de trabalho. A pausa deve ser ativa (caminhando, alongando-se) para quem fica muito sentado.

– Participe da Ginástica Laboral com entusiasmo, realizando os movimentos em toda sua amplitude, pois isto propicia um aumento do fluxo sanguíneo e remoção de toxinas produzidas pelo esforço.

– Ao atender ao telefone, faça apenas isto. Caso precise anotar algo ou consultar algo no computador, nunca prenda o telefone entre o ombro e ouvido.

8. Conceitos

Para os efeitos desta política, aplicam-se os seguintes termos e definições:

– *Ativo:* todas as coisas que tem valor para a empresa;

– *Informação:* ativo resultante do processamento, manipulação e organização de dados, que representa uma modificação no conhecimento do sistema que a recebe. Ativo de grande importância para a organização;

– *Segurança da Informação:* é a proteção da informação de vários tipos de ameaça para garantir a continuidade do negócio; é a preservação da

autenticidade, confidencialidade, integridade e da disponibilidade da informação;

- *Política de Segurança da Informação:* definição de normas e procedimentos, ferramentas e responsabilidades, que visam minimizar os riscos dos ativos (informação) de uma organização;
- *Autenticidade:* garantir que a informação é procedente da fonte informada em seu conteúdo;
- *Disponibilidade:* consiste em assegurar um acesso seguro e confiável à determinada informação por um usuário autorizado;
- *Integridade:* é garantir que a informação manipulada mantenha as características originais, que foram estabelecidas pelo proprietário da mesma;
- *Confidencialidade:* evitar que ela seja acessada por um usuário que não tenha permissão do proprietário em qualquer tipo de acesso na mesma.

9. Definições para a classificação das informações

Deve-se classificar a informação para indicar a necessidade, prioridades e o nível esperado de proteção quando do tratamento da informação (NBR ISO/IEC 27002, item 7.2).

A informação deve ser classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização (NBR ISO/IEC 27002, item 7.2.1).

Cada departamento deverá estipular o nível de confidencialidade de suas informações, onde tal atividade deverá ser realizada pelo gestor da área (Gerente, Supervisor e/ou Líder). O nível de confidencialidade deverá ser definido conforme os conceitos abaixo:

- *Secreta:* são informações de extrema importância para a organização, por isso devem ser acessadas por um número restrito de pessoas sendo totalmente controladas sobre a utilização de tais informações.
- *Confidencial:* é toda informação que pode ser acessada pelos membros e parceiros da organização, porém, a divulgação não autorizada das mesmas pode causar danos irreparáveis à organização, no âmbito financeiro como também no relacionamento com clientes.
- *Interna/Pública:* são informações que devem ficar disponíveis apenas para a organização, podendo ser acessada por todos os membros, porém, deve-se evitar o acesso externo das mesmas.

Cabe ao gestor da área, juntamente com a presente política, a responsabilidade de conscientizar seus subordinados sobre os cuidados e a correta utilização das informações, os quais deverão estar compromissados em não deixar qualquer tipo de mídia confidencial e/ou relatório exposto em impressoras, sobre mesas ou abertos em suas estações de trabalho quando estiverem ausentes, de modo a evitar o acesso não autorizado às informações por outros indivíduos.

10. Definições para Usuário e Senha de Acesso à Rede

Cada usuário deve utilizar um identificador (ID/Login de usuário) único para assegurar sua responsabilidade para com suas ações (NBR ISO/IEC 27002, item 11.2.1). Este identificador de usuário é gerado e liberado pela Informática após solicitação e aprovação.

O uso de identificadores (Login) em grupo só será permitido por razões operacionais ou por real necessidade do negócio, e perante aprovação (NBR ISO/IEC 27002, item 11.2.1).

10.1 Os dados de autenticação (usuário e senha) deverão ser aprovados pelo gestor da área solicitante e/ou por um membro da gerência geral, através do Sistema de Gerenciamento da Informática, o Help Desk da

organização, para solicitação do recurso pelo usuário e Solicitação de Acesso para aprovação do gestor e membros da gerência geral.

10.2 A senha de acesso deverá ter o tamanho mínimo de 8 caracteres.

10.3 Deverá de modo automático e gerenciado pelo sistema, ser efetuada a troca da senha a cada 120 dias.

10.4 Poderá ser utilizada até 6 conexões após a senha ter expirado (gerenciado pelo sistema).

10.5 Deverá ser cadastrada, quando solicitada a substituição, senha diferente das últimas 5 utilizadas pelo usuário (gerenciado pelo sistema).

10.6 Deverá de modo automático e gerenciado pelo sistema, ser efetuada a substituição da senha inicial definida pelo administrador da rede por uma senha pessoal e intransferível, exceto no caso de usuários públicos, que são utilizados por segmentos como portaria, usuários de sistemas específicos da empresa (Ems, Data Ponto, Webdesk, entre outros); Os usuários destes recursos compartilhados também estão comprometidos a não divulgarem sua senha para membros que não estiverem enquadrados nestes grupos.

10.7 Deverá, em qualquer hipótese, manter sigilo absoluto da senha, sendo sujeito às penalidades previstas no item X da presente Política.

10.8 Deverá ser evitada a utilização de senhas seqüenciais (Ex.: 123 ou abc) e/ou senhas de fácil dedução, de modo a dificultar que intrusos tentem adivinhar as senhas dos usuários.

10.9 As senhas para usuários com perfil de administrador da rede deverão ficar sob a guarda do supervisor da área de Redes e Aplicativos, da gestora do departamento de Informática e, ainda no caso da senha dos administradores corporativos, também os analista responsáveis e, no caso das senhas de administrador local da unidade sob a tutela do analista residente (nas unidades onde não houver analista residente, um supervisor terá acesso a esta senha).

10.10 Os usuários finais, não poderão ter acesso de administrador nas estações de trabalho. Tal recurso só será utilizado pela equipe de TI, facilitando e padronizando o perfil e manutenção das estações.

11. Definições de Direitos de Acesso às Informações

Não será permitida a liberação de acessos que não são necessários para a execução das atividades de um determinado colaborador. Deve-se solicitar somente o necessário.

O nível de acesso concedido ao usuário deve sempre ser apropriado ao propósito do negócio (NBR ISO/IEC 27002, item 11.2.1).

Todo e qualquer ativo deverá possuir um proprietário responsável por ele (criador, utilizador, etc.), para que este participe efetivamente dos processos e atividades de segurança da informação para com este ativo.

Deve-se evitar a exposição de documentos com informações sensíveis e confidencias sobre mesas, impressoras, telas e emails.

11.1 O administrador da rede antes de definir direito de acesso a pastas e arquivos da rede a qualquer usuário deverá verificar o seguinte:

- Todas as atribuições deverão ser solicitadas através do Help Desk da Informática e aprovadas através de Solicitação de Acesso (documento auxiliar).

11.2 Direito de acesso a pasta(s) ou arquivo(s) pertencente(s) a departamentos diferentes da lotação do usuário que necessita:

- Deverá ser aprovado pelo gestor da área e/ou por um membro da gerência geral.

11.3 Direito de acesso a pasta(s) ou arquivo(s) pertencente(s) a gestores, gerência geral ou diretoria:

- Deverá ser aprovado por um membro da gerência geral (pastas deste nível) e/ou diretoria (pastas de ambos os níveis).

12. Definições para a utilização dos recursos de TI

Todos os colaboradores deverão estar cientes da importância da notificação imediata de qualquer tipo de fragilidade identificada em qualquer sistema e/ou serviço da informação (NBR ISO/IEC 27002, item 13.1.2).

A empresa poderá inspecionar qualquer arquivo ou programa armazenado na rede ou fora dela, estejam nas áreas privadas da rede, hard disk e discos removíveis das estações de trabalho.

Não será permitido a qualquer colaborador ou contratado:

12.1 Expor, copiar, armazenar, distribuir, editar ou gravar através do uso dos recursos computacionais da rede corporativa, material sexualmente explícito.

12.2 Utilizar-se dos recursos de Tecnologia da Informação da empresa para atividades ilegais.

12.3 Fazer *download* (cópia para dentro) de software ou a execução de cópias não autorizadas, em computadores dentro da empresa, pois esta ação caracteriza a “Pirataria Corporativa”, que mesmo realizada em pequenas quantidades, pode significar multas e pena de detenção, estabelecidas na Lei 9.609/98 (Lei de Programas de Computador).

12.4 Utilizar-se dos recursos de Tecnologia da Informação da empresa para invadir sistemas de terceiros.

12.5 Utilizar-se dos recursos de Tecnologia da Informação da empresa para deliberadamente propagar qualquer tipo de vírus, worms (programas que se propagam automaticamente), cavalos de tróia (programas que executam funções maliciosas) e backdoors (programas para controle de outros computadores).

12.6 Acessar, participar e divulgar informações em sites de Bate-Papo ou Grupos de Discussão, em nome da empresa ou não.

12.7 Fazer download (cópia para dentro) de quaisquer softwares de entretenimento ou jogos através dos recursos de Internet.

12.8 Acessar e participar de sites de entretenimento e jogos contra oponentes, utilizando os recursos de Internet ou qualquer outro recurso de Tecnologia de Informação da empresa.

12.9 Em qualquer forma, efetuar upload (cópia para fora) de qualquer software ou sistema licenciado à empresa, ou de dados de propriedade da empresa ou de seus clientes e fornecedores.

12.10 Divulgar ou emprestar seu código de identificação e sua senha de acesso à internet ou a rede e e-mail, pois todas são pessoais e confidenciais.

12.11 Realizar tentativas de alteração de parâmetros dos equipamentos ou softwares que protegem a nossa rede interna ou externa.

12.12 Enviar, transmitir ou disponibilizar em qualquer forma, mensagens do tipo pirâmide, corrente ou qualquer outro tipo de apelo, que cresçam em progressão geométrica.

12.13 Distribuir qualquer mensagem ou arquivo com o objetivo de difamar, insultar ou ensejar constrangimento relacionado à discriminação por raça, sexo, origem, cor, idade, condição social, porte de deficiência, incapacidade e crença política, religiosa e esportiva.

12.14 Tentar obter acesso não autorizado de contas de administradores ou de qualquer outra conta não pertencente ao usuário.

12.15 Acessar ou tentar acessar as mensagens de correio eletrônico recebidos por terceiros.

13. Definições para instalação e uso de softwares

Todo e qualquer tipo de software deverá e poderá ser instalado apenas pela equipe da área de TI, de modo a evitar o uso de programas ilegais (Piratas) dentro da organização.

A empresa possui licenças para uso de determinados softwares, proveniente de uma série de fornecedores. Não somos autores destes softwares ou de sua

documentação. Portanto, exceto quando autorizado pelos autores do software, nenhum colaborador ou contratado tem o direito de reproduzi-lo.

13.1 A equipe de TI verificará periodicamente os dados dos computadores e servidores, realizando inventários de software para evitar o uso do programas ilegais e também monitorar o número de licenças dos programas legais que estão sendo utilizados.

13.2 A necessidade de utilização de um novo software deverá ser solicitada através do SGI Help Desk com sua respectiva justificativa. Tal solicitação além de aprovada deverá ser analisada (preço do software, compatibilidade, recursos necessários, e outros).

13.3 O colaborador ou contratado que tomar conhecimento de algum uso inadequado de software da empresa ou de sua respectiva documentação dentro ou mesmo fora da empresa deverá notificar o gerente do departamento ou a consultoria jurídica da empresa.

13.4 De acordo com a Lei 9.609/98, as pessoas envolvidas em reprodução ilegal de programas ficam sujeitas ao pagamento das respectivas indenizações por perdas e danos, em valor correspondente a até duas mil vezes o valor de cada cópia do programa original, além de sanções penais como multas e prisão.

13.5 O Colaborador ou contratado que copiar, adquirir ou usar cópia ilegal e não autorizada, fica inteiramente responsável pela reparação dos danos resultantes de tais atos

14. Definições para admissão, demissão e transferência de funcionários

As responsabilidades pela segurança da informação devem ser atribuídas antes da contratação, de forma adequada, nas descrições de cargo e nos termos e condições de contratação (NBR ISO/IEC 27002, item 8.1).

Todos os candidatos ao emprego, fornecedores e terceiros devem ser adequadamente analisados, especialmente em cargos com acesso a informações sensíveis (NBR ISO/IEC 27002, item 8.1).

Todos os funcionários, fornecedores e terceiros, usuários dos recursos de processamento da informação devem assinar acordos sobre seus papéis e responsabilidades pela segurança da informação (NBR ISO/IEC 27002, item 8.1).

14.1 O setor de Recrutamento e Seleção deverá informar ao setor de informática qualquer movimentação de funcionários que tenham ou terão cadastro de utilização dos recursos de TI, para que as liberações, bloqueios e treinamentos necessários sejam realizados para o funcionário.

14.2 No caso de uma transferência de funcionário, o setor de informática deverá ser comunicado imediatamente para que as adequações de acesso do funcionário sejam realizadas.

14.3 Cabe ao setor de RH obter as assinaturas necessárias de concordância em relação a esta política.

14.4 Os gestores de cada área terão a responsabilidade de enfatizar a prática da segurança da informação em seus setores de acordo com o estabelecido na presente política.

14.5 Todo novo colaborador usuário dos recursos de processamento da informação deve ser treinado nas diretrizes da segurança da informação, tomando como base a presente política.

14.6 Havendo rescisão do contrato de trabalho ou rescisão do contrato de terceirização de atividades, o setor responsável, juntamente com o setor de RH, deverão informar a área de TI para que as permissões e/ou acessos liberados sejam cancelados.

15. Definições para o uso de internet

O uso da internet na CMNP é considerado uma concessão e não um direito, além de ser considerado como uma conexão de alto risco, por isso se faz necessária a conscientização e aplicação de regras para os usuários que têm ou terão acesso a internet.

15.1 O acesso a internet será liberado apenas para os colaboradores que dependem de tal acesso para executar suas funções, e esta liberação só poderá ser feita diante da aprovação do gestor do colaborador.

15.2 Com os mecanismos de autenticação da área de TI, todo acesso de todos os colaboradores serão monitorados e armazenados nos servidores e serão gerados relatórios com os sites acessados para possíveis averiguações.

15.3 A utilização deste recurso deve ser totalmente relacionada aos objetivos da empresa. Quando necessário, os colaboradores que precisarem realizar acessos não relacionados com os objetivos da empresa, deverão fazê-los em horários que sejam fora do expediente (almoço).

15.4 É extremamente proibida a divulgação de informações da empresa em fóruns e/ou listas de discussões.

15.5 Com exceção dos colaboradores com cargos de Gerentes e Diretores, os downloads de arquivos serão bloqueados para todos os outros usuários. Quando for necessário o download de algum tipo de arquivo ou ferramenta, este deverá ser solicitado ao setor de TI via SGI Help Desk.

15.6 Não é permitido a acesso a sites pornográficos, de entretenimento, de relacionamentos (Orkut, MSN), sites de jogos e outros.

15.7 O uso de sites de notícias ou de pesquisa será aceitável, desde que o seu uso não comprometa o bom andamento dos trabalhos.

15.8 Serão de total responsabilidade do colaborador todos os acessos realizados através de seu login.

15.9 A empresa poderá a qualquer momento, bloquear o acesso a internet do colaborador, caso tenha suspeita de mau uso deste recurso.

Obs.: se por eventualidade o acesso a algum site estiver bloqueado, e este for necessário para o desenvolvimento de atividades para a empresa e ainda atende a esta política, o desbloqueio deve ser solicitado ao setor de TI via SGI Help Desk.

16. Definições para o uso de Correio Eletrônico (email)

O correio eletrônico fornecido pela CMNP é o Novell GroupWise, sendo este uma ferramenta que deverá ser utilizada para facilitar a comunicação entre colaboradores e terceiros, fornecendo também agilidade no fluxo de informações úteis para tomadas de decisão, economia com custos em materiais de escritório (papel, caneta, etc.), e alta confiabilidade (dados enviados e recebidos são registrados, sendo inalteráveis para fins de fiscalização).

Para uma melhor utilização do Correio Eletrônico, convém que:

16.1 O uso do recurso de correio de eletrônico é pessoal e intransferível, sendo que todas as mensagens enviadas são de responsabilidade do usuário da conta de email.

16.2 Os textos e arquivos enviados pelo correio eletrônico deverão estar de acordo com a visão ética e profissional da empresa, evitando a utilização de linguagens informais que comprometam e imagem da organização.

16.3 É terminantemente proibido o envio de emails tipo corrente, com linguagem ofensiva ou difamatória, com conteúdos pornográficos ou equivalentes e/ou que prejudiquem direta ou indiretamente pessoas e a empresa.

16.4 Recomenda-se que os emails internos e/ou externos de origem desconhecida que contenham links para acesso devem ser removidos ou enviados para análise da equipe de TI, sendo que os mesmos possam vir a ser vírus ou spam.

16.5 É importante que figuras não sejam coladas diretamente no corpo do e-mail ou nos chamados do SGI Help Desk, via Print Screen de telas, ou via comando de copiar e colar tabelas do Word ou Excel, pois estes geram mensagens muito grandes e não são possíveis de visualizar seus tamanhos antes de enviar. **Recomendação:** colar as figuras geradas via print screen ou cópia de tabelas, em documento Word e gerar um arquivo a parte, para acompanhar o tamanho e anexar se estiver adequado.

16.6 Existem recursos no GroupWise que permitem o compartilhamento de mensagens em caixas de email específicas, a partir de regras (configurações e/ou direito de Proxy), portanto sempre que necessário deverá ser utilizado este meio, quando aplicável, evitando replicação para vários usuários que necessitam conhecer o assunto. Somente o proprietário da caixa de e-mail pode criar regras para permitir o compartilhamento ou automatizar encaminhamentos, portanto cabe ao mesmo cuidar das regras ativas e dos direitos de acesso liberados, pois é de sua total e exclusiva responsabilidade manter as caixas somente com os conteúdos necessários a empresa e aos usuários que terão o acesso compartilhado.

16.7 Proceder toda semana ou no mínimo uma vez por mês, a transferência de e-mails já tratados e/ou mais antigos e de interesse da empresa que não podem ser excluídos para o "Arquivo Reserva" (servidor alternativo de backup de emails), para que sejam efetuados os processos de backup.

16.8 A empresa poderá a qualquer momento, bloquear a utilização da conta de email, caso tenha suspeita de mau uso destes recursos.

17. Definições para o uso de Antivírus

A proteção contra códigos maliciosos deve ser baseada em software de detecção de códigos maliciosos e reparo, na conscientização da segurança da informação e no controle de acesso adequado (NBR ISO/IEC 27002, item 10.4.1).

A CMNP utiliza antivírus e ferramentas afins da Kaspersky para proteção das estações de trabalho e dos servidores.

Para a utilização eficaz deste recurso na CMNP, convém que:

17.1 Todos os computadores devem ter suas entradas USB's, unidade de disquete e CD-ROM bloqueados pelo antivírus, com exceção dos computadores da equipe de TI.

17.2 É de responsabilidade da área de TI todo e qualquer tipo de cópia e/ou gravação de arquivos para dentro ou fora da rede corporativa.

17.3 Todo e qualquer tipo de arquivo de dispositivos e mídias removíveis (Pendrives, CDs, DVDs, Cartões, e outros) devem ser verificados pelo programa de antivírus antes de qualquer ação.

17.4 Todas as estações de trabalho e servidores devem ter instalado o programa de antivírus, sem nenhuma exceção, e a atualização de produto deve ser realizada de forma automática.

17.5 A equipe de TI tem a responsabilidade de gerenciar todos os dispositivos protegidos pelo programa de antivírus, verificando relatórios e tomando ações quando necessário.

17.6 Com exceção da equipe de TI, os usuários são "inaptos" a alterar as configurações e/ou desabilitar o antivírus de suas estações.

18. Definições para cópias de segurança (backup)

As cópias de segurança das informações e dos softwares devem ser efetuadas e testadas regularmente conforme a política de cópias de segurança definida (NBR ISO/IEC 27002, item 10.5.1).

Com objetivo de garantir a integridade dos dados, a realização do backup dos dados da CMNP ocorre diariamente, mensalmente e anualmente.

18.1 *Backup Diário:* realizado diariamente no modo DIFERENCIAL, onde o sistema cria uma cópia de segurança dos arquivos que sofreram modificações após o último backup FULL (total);

18.2 *Backup Mensal:* realizado no último dia de cada mês e no primeiro dia útil do mês subseqüente, no modo FULL (total) copiando para a mídia externa todos os arquivos da rede;

18.3 *Backup Anual:* realizado no último dia de cada ano e no primeiro dia útil do ano subseqüente, no modo FULL (total) copiando para a mídia externa todos os arquivos da rede.

18.4 Os backups *diários* são mantidos por um período de 30 dias, os *mensais* são descartados após 12 meses e os backups *anuais* não são descartados, uma vez que, conforme levantamentos realizados junto a algumas áreas do grupo existem dados que não poderão ser descartados e que, eventualmente, precisarão ser restaurados, seja por motivos de consulta de histórico, ou levantamento de documentos requeridos por ações judiciais, ou qualquer outro que vier a ocorrer.

19. Definições para acessos e recursos físicos

Devem ser utilizados perímetros de segurança para proteger as áreas que contenham informações e instalações de processamento da informação (NBR ISO/IEC 27002, item 9.1.1).

As áreas seguras devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso (NBR ISO/IEC 27002, item 9.1.2).

19.1 Não será permitida a entrada de pessoas de outras áreas na sala dos servidores e de manutenção de TI. Tal acesso só será permitido com acompanhamento de um dos membros da equipe de TI.

19.2 Qualquer necessidade de manutenção nas caixas de fibra óptica deve ser comunicada ao setor de TI para que seja realizado um acompanhamento pelo membro responsável da equipe.

Os equipamentos devem ser protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades (NBR ISO/IEC 27002, item 9.2.2).

O cabeamento de energia e de telecomunicações que transporta os dados ou dá suporte aos serviços de informações deve ser protegido contra interceptação ou danos (NBR ISO/IEC 27002, item 9.2.3).

19.3 E terminantemente proibido a abertura ou manutenção de equipamentos de informática por usuários que não são do setor.

19.4 Todos os equipamentos de TI estão ligados em No-breaks para evitar qualquer dano ou perda nos trabalhos realizados em casos de falta de energia.

19.5 Todo cabeamento relacionado à comunicação de dados estão instalados em linhas diferentes para evitar interrupções ou interferências com outras linhas.

20. Penalidades

O descumprimento das normas estabelecidas nesta política ou outras que vierem a ser implantadas serão punidos, na conformidade das penalidades abaixo, observando-se para aplicação das mesmas a natureza e a gravidade do ato faltoso:

20.1 Colaboradores:

- Advertência por escrito;
- Suspensão do trabalho por 3 (três) dias, acrescidos da perda do D.S.R. (Descanso Semanal Remunerado);
- Demissão por justa causa.

20.2 Contratados (fornecedores/terceiros):

- Rescisão contratual ou;
- Execução e demais penalidades previstas em Lei;

Apêndice B – QUESTIONÁRIO APLICADO AOS USUÁRIOS DE TI DA CMNP

1	**As informações que você necessita estão sempre disponíveis?**	
	Sim	5
	Às vezes	2
	Não	2
2	**Como avaliaria a segurança das informações que você trabalha?**	
	Ótimo	2
	Regular	4
	Ruim	3
3	**Você tem conhecimento de suas limitações de acesso a internet?**	
	Sim	1
	Algumas	5
	Não	3
4	**Você necessita e utiliza todas as pastas que têm acesso?**	
	Sim, todas	1
	Quase todas	5
	Quase nenhuma	3
5	**Conhece documentos formalizando as restrições da área de TI?**	
	Sim	1
	Ouviu Falar	2
	Não	6
6	**Os arquivos utilizados em conjunto estão sempre íntegros e atualizados?**	
	Sim	2
	Não	3
	Não Aplicável	4
7	**Seu gestor está envolvido com suas necessidades de utilização da informação?**	
	Sim, completamente	3
	Pouco	2
	Não	4
8	**Uma segunda pessoa tem conhecimento de sua senha de email ou de login?**	
	Sim	4
	Já teve	1
	Não	4
9	**Deixa documentos e/ou relatórios sobre mesas, impressoras ou abertos em tela?**	
	Sim	5
	Deixava	1
	Não	3
10	**Conhece as penalidades que podem ser aplicadas pelo mau uso da informação?**	
	Sim	1
	Algumas	2
	Não	6

Apêndice C - USUÁRIOS PARTICIPANTES DO QUESTIONÁRIO

Recursos Humanos

Nome:	Colaborador 01
Setor:	Recursos Humanos
Cargo:	Analista de Recursos Humanos Junior
Nome:	Colaborador 02
Setor:	Recursos Humanos
Cargo:	Analista de Recursos Humanos Pleno
Nome:	Colaborador 03
Setor:	Recursos Humanos
Cargo:	Auxiliar Administrativo

Contabilidade

Nome:	Colaborador 04
Setor:	Contabilidade
Cargo:	Analista Contábil Pleno
Nome:	Colaborador 05
Setor:	Contabilidade
Cargo:	Analista Contábil Pleno
Nome:	Colaborador 06
Setor:	Contabilidade
Cargo:	Assistente Contábil

Desenvolvimento Agrícola

Nome:	Colaborador 07
Setor:	Desenvolvimento Agrícola
Cargo:	Assistente Administrativo
Nome:	Colaborador 08
Setor:	Desenvolvimento Agrícola
Cargo:	Analista Administrativo
Nome:	Colaborador 09
Setor:	Desenvolvimento Agrícola
Cargo:	Assistente Administrativo