1. **Política de Segurança da Informação**

**6.1** Acessos

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Contas de Usuário | Nome Completo | Setor / Grupo | Cargo | Atribuições/ Funções |
| MARIAS | Maria Silva | Diretoria | Diretora Geral | FileServer |
| MARIOC | Mario Carvalho | Comercial | Gerente Comercial | FileServer |
| ROBSONJ | Robson de Jesus | TI | Analista Infraestrutura | Zabixx, Diretoria, FileServer, TI, Server Dev-Hom, Server Prod, Desenvolvimento |
| JOSEO | José Maria de Oliveira | Engenharia | Engenheiro | FileServer |
| RUBENSN | Rubens Alfredo Neto | Financeiro | Analista Financeiro | FileServer, Server Dev-Hom, Server Prod, Desenvolvimento |
| MATHEUSK | Matheus Kuno | TI | Gerente de TI | Zabixx, Diretoria, FileServer, TI, Server Dev-Hom, Server Prod, Desenvolvimento |
| FELIPES | Felipe Siementkowski | TI | Gerente de TI | Zabixx, Diretoria, FileServer, TI, Server Dev-Hom, Server Prod, Desenvolvimento |
| DIEGOR | Diego Felipe Reynoud | TI | Desenvolvimento | Zabixx, Diretoria, FileServer, TI, Server Dev-Hom, Server Prod, Desenvolvimento |
| CLAUDIOL | Cláudio Maurício de Lima | Recursos Humanos | Gerente de RH | FileServer |

**6.2** Pilares da Segurança

* Confidencialidade ou sigilo – somente as pessoas autorizadas possam utilizar certas informações transmitidas;
* Disponibilidade – A informação deve estar disponível no momento em que a mesma for solicitada;
* Autenticidade – garantia que a comunicação é autêntica, ou seja, as entidades envolvidas são realmente quem dizem ser;
* Integridade – garantir que o conteúdo de uma mensagem não será alterado durante seu tráfego;
* Não recusa – garantir que o emissor de uma mensagem não poderá posteriormente negar sua autoria; e
* Controle de Acesso – regras de autenticação para cada usuário ou grupo de usuário.

**6.3** Política de Segurança de Usuário (PSU)

Para o usuário deve ser implantado a PSU, que é um conjunto de normas para apontar aos usuários os principais pontos da Política de Segurança da Informação pertinentes às responsabilidades e direitos deles e da organização. A PSU deve ser objetiva, sendo utilizada para registrar o aceite do usuário, evitando a informalidade do processo, fato que pode levar o usuário a não cumprir o seu papel. Devem ser incluídas na política de segurança algumas determinações quanto à conformidade e execução, que definem o que deve acontecer quando a segurança é violada. Conforme a empresa cresce, as tecnologias evoluem, por isso faz-se necessário que os documentos sobre as políticas de segurança mantenham revisões periódicas, de modo a garantir que eles estejam sempre atualizados e sejam aderentes às necessidades da empresa.

**6.4** Estudo da Elaboração da Política de Segurança

Para criação de uma política de segurança deve-se verificar as especificidades da empresa em questão. Portanto são estabelecidas neste documento normas de utilização e atividades que são entendidas de violação ao uso dos serviços e recursos, os quais são considerados proibidos. Esta Política de Utilização de Rede é um documento normativo interno, com valor jurídico e aplicabilidade imediata, plena e indistinta, devendo ser seguida obrigatoriamente, por todos os colaboradores da empresa, incluindo empregados, prestadores de serviço, fornecedores, parceiros, estagiários ou quaisquer indivíduos (independentemente de seu nível hierárquico ou atividades que desempenhem) ou entidades que de algum modo, participem dos processos de negócio da mesma ou tenham acesso às suas informações, estendendo-se também, a todos os processos automáticos criados ou conduzidos para gestão dos sistemas disponíveis. Neste documento deve estar explícito as responsabilidades de cada setor envolvido ao empregado e quem deverá aplicar e gerenciar a política e monitorar, como, por exemplo:

**6.5** Departamentos:

**6.5.1** A empresa será responsável pela inserção de avisos legais nas interfaces de uso de seus sistemas e rede para orientação de conduta dos colaboradores. Estes avisos têm finalidade educativa.

**6.5.2** O Departamento de RH (Recursos Humanos) é responsável em informar aos novos colaboradores quando contratados, sobre este procedimento e coletar as assinaturas necessárias no documento e definição dos colaboradores auditados mensalmente;

**6.5.3** O usuário é responsável pela utilização correta e ética da rede conforme descrito neste procedimento. Quando em dúvida sobre o que é considerado, de alguma forma, violação, deverá contatar o departamento de recursos humanos;

**6.5.4** O Departamento de TI (Tecnologia da Informação) é responsável por implementar e monitorar o cumprimento desta determinação, sendo que quando da necessidade de alteração de algum fato, comunicará em tempo hábil todos os envolvidos. Para garantir que as normas sejam cumpridas será necessário a verificação periódica. O Departamento de TI deve acompanhar e verificar o cumprimento da política de utilização da rede, estes são realizados através de:

* Implementação de *softwares* e sistemas que monitoram e gravam todos os usos de *Internet* através da rede e das estações de trabalho da empresa e somente os que forem autorizados pela empresa poderão ser utilizados pelos colaboradores e parceiros;
* Inspecionando qualquer arquivo armazenado na rede, esteja no disco local da estação ou nas áreas privadas da rede, visando assegurar o rígido cumprimento desta política;
* Instalando uma série de *softwares* e *hardwares* para proteção da rede interna e garantia da integridade dos dados e programas, incluindo um *firewall* que é a primeira, mas não a única barreira entre a rede interna e a *Internet*;
* Realizado o monitoramento dos serviços de mensagem corporativo em uso, como por exemplo: *Outlook*/*Exchange* para o *e-mail*.
* Proibindo a utilização de *CDs/DVDs, Pen Drives* e afins, vindos de fora da empresa, sem verificação e aprovação do seu conteúdo pelo Suporte Técnico da TI;
* Proibindo a utilização de *notebooks* particulares ou terceirizados sem que seja feita varredura por programa antivírus padrão utilizado pela empresa. Esta verificação poderá ser efetuada sempre que for necessária, não acontecendo somente uma vez.
* Implementação de *softwares* e sistemas que monitoram e gravam todos os usos de *Internet* através da rede e das estações de trabalho da empresa e somente os que forem autorizados pela empresa poderão ser utilizados pelos colaboradores e parceiros;

O usuário ainda, deve estar ciente que pode ser submetido a este acompanhamento e essas informações devem constar no documento oficial entregue a ele. As normas permitindo ou considerando o que seria uma violação, devem ser divididas de acordo com a necessidade da empresa, de forma geral é possível que algumas dessas divisões sejam:

Utilização da rede; Utilização de *E-Mail;* Utilização de Impressoras; Acesso à *Internet;* A utilização da rede deve englobar definições para uso da rede desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

E algumas normas como: Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede; Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com sessão de usuários, principalmente se não tiver sido autorizado pelos responsáveis de TI;  Realizar periodicamente a manutenção no diretório pessoal, evitando acúmulo de arquivos inúteis e a capacidade máxima ofertada a cada usuário deverá ser respeitada; Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas acessados, evitando, desta maneira, o acesso por pessoas não autorizadas e sempre efetuar o *logout/logoff* da rede ou bloqueio do *desktop* através de senha; Materiais de natureza pornográfica e racista não podem ser acessados, expostos, armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais da rede, sendo possível aplicar as penalidades previstas nas políticas e procedimentos internos.

Em “Utilização do *e-mail*” devem constar normas que englobam toda a relação do usuário com seu *e-mail*, o envio, recebimento e gerenciamento de sua(as) conta(as):

* É proibido enviar *e-mail* a terceiros contendo informações confidenciais;
* É proibido reenviar ou de qualquer forma propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;
* É proibido forjar qualquer das informações do cabeçalho do remetente;
* Não é permitido má utilização da linguagem em respostas aos *e-mails* comerciais, tais abreviações de palavras (Ex.: ¨vc¨ ao invés de ¨você¨, “beijos” ao invés de “abraços”);
* Não é permitido envio de *e-mail* impróprio, obsceno, que atente à moral e aos bons costumes ou que não seja compatível com os padrões de conduta ética aceitos pela empresa;
* Não receber e não enviar mensagens (internas ou externas) contendo anexo(s) superior(es) a 10 *MegaBytes;*
* É obrigatória a utilização de assinatura nos e-mails conforme configuração efetuada pelo TI. Exemplo: “Nome do Colaborador”, “E-mail do colaborador”, “Empresa”, “Endereço”, “Telefone Comercial” e “Site: http://www.empresa.com.br”.

Em “Utilização da Impressora” deve ser definido normas para utilização das impressoras disponíveis no interior da empresa. Sendo algumas delas:

* Ao mandar imprimir, verifique na impressora se o que foi solicitado já está impresso, para não haver impressões "sem dono" acumulando-se;
* Não é permitido deixar impressões erradas na mesa das impressoras, na mesa das pessoas próximas a ela e tampouco sobre o gaveteiro;
* Utilize a impressora colorida (caso haja) somente para versão final de trabalhos e não para testes ou rascunhos;
* Não é permitida impressão particular, sem prévia autorização da coordenação, sendo que cópias particulares serão cobradas;
* Não é permitido o reaproveitamento de páginas já impressas que contenham informações da empresa.

Em “Acesso à *internet*” visa definir as normas de utilização da *Internet* que engloba desde a navegação a sites, *downloads* e *uploads* de arquivos. Neste tópico as normas devem ser especialmente claras para que não haja dúvidas em relação ao seu uso, levando em consideração que a *internet* é utilizada a maior parte do tempo pelos usuários. Algumas das possíveis normas são:

* É proibido utilizar os recursos da empresa para fazer o *download* ou distribuição de *software* ou dados não legalizados;
* É proibida a divulgação de informações confidenciais da empresa em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;
* Pode ser utilizada a *Internet* para atividades não relacionadas com os negócios durante o horário de almoço, ou fora do expediente (somente nestes horários), desde que dentro das regras de uso definidas nesta política;
* Os colaboradores com acesso à *Internet* podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas, como também a correta instalação;
* Colaboradores com acesso à *Internet* não podem efetuar *upload* de qualquer *software* licenciado à empresa ou de dados de propriedade da empresa ou de seus clientes, sem expressa autorização do gerente responsável pelo *software* ou pelos dados;
* Caso a empresa julgue necessário poderá bloquear o acesso aos arquivos e domínios que comprometam o uso de banda de *internet* ou perturbe o bom andamento dos trabalhos;
* São gerados relatórios dos sites acessados por usuário e se necessário à publicação dos mesmos;
* É obrigatório a utilização de um *browser* específico (ex: *Firefox*), ou outro *software* homologado pelo departamento técnico para ser o cliente de navegação;
* Não é permitida a utilização de serviços de *streaming*.
* Não é permitido jogos *on-line* ou *stand alone* (sem conexão de *internet*);
* Não é permitido a utilização de qualquer tipo de sistema de camuflagem de navegação, deletar o histórico de navegação ou de desvio de *proxy*.
* Não é permitido quaisquer *softwares*, aplicativos, ferramentas, arquivos e *plugins* de origem duvidosa, pirata e/ou não homologados previamente pelo Departamento de Informática.

**6.6** Política de Utilização de Rede

A política de utilização de rede desta empresa assegura um serviço de rede de alta qualidade através de comportamento ético e profissional dos usuários de rede; portanto são estabelecidas normas de utilização e atividades que são entendidas de violação ao uso dos serviços e recursos, os quais são considerados proibidos. Esta política é um documento normativo interno, com valor jurídico e aplicabilidade imediata, plena e indistinta, devendo ser seguido obrigatoriamente, por todos os colaboradores da empresa, incluindo empregados, prestadores de serviço, fornecedores, parceiros, estagiários ou quaisquer indivíduos (independentemente de seu nível hierárquico ou atividades de desempenhem) ou entidades que de algum modo, participem dos processos de negócio da mesma ou tenham acesso às suas informações, entendendo-se, também, a todos os processos automáticos criados ou conduzidos para gestão dos sistemas disponíveis. As principais orientações sobre as regras de utilização dos recursos de informática estão descritas abaixo, cabe ao colaborador fazer uso adequado dos equipamentos de informática e dos softwares disponibilizados pela empresa. Demais orientações estão descritas na Política de Utilização de Rede e o cumprimento da Política é obrigatório; o não cumprimento ou a recusa em fazê-lo implica em sanções disciplinares e/ou trabalhistas.

Devendo ter em mente os seguintes objetivos:

* A T.I (Tecnologia da Informação) é responsável pela instalação de *hardware* e *software* para os usuários; bem como prestar atendimento e suporte quando necessário.
* Não é permitido que o usuário realize alterações na configuração dos equipamentos e *softwares*, sendo que todas as modificações devem ser solicitadas a T.I., evitando problemas causados pelo uso indevido.
* É proibido a manipulação e armazenamento de arquivos, fotos, músicas e vídeos que não estejam relacionados com as atividades do usuário na empresa e/ou contenham direitos autorais.
* Quando o colaborador acessar a *Internet*, torna-se responsável por todas as atividades geradas pelo seu acesso, incluindo mensagens, comandos, programas, *softwares* ou arquivos gerados ou recebidos.

* A empresa condena o uso ilegal, antiético, não autorizado ou prejudicial da *internet*, o que inclui não só o acesso, transmissão e armazenamento de pornografia, mas também de conteúdos considerados impróprios, ou ofensivos e depreciativos em relação à idade, raça, sexo, religião, nacionalidade, deficiência física ou orientação sexual.
* Todos os *e-mails* recebidos pelos usuários e mensagens instantâneas recebidas e enviadas terão auditoria da T.I, assim como todas as páginas visitadas terão seus endereços registrados e ficarão à disposição da Diretoria.
* O *e-mail* é uma ferramenta extremamente útil e poderosa para comunicação, devendo ser utilizado de forma produtiva, evitando o mau uso. Sendo proibido o envio ou retransmissão para outros (internos ou externos) referente a:

Avisos de novos vírus e *e-mail;* Correntes para ganhar dinheiro fácil; Campanhas de ajuda a pessoa enfermas/desaparecidas; Abaixo-assinado sobre guerras e situações políticas; Participação de promoção de vendas e/ou concurso; Promover, colaborar ou divulgar *SPAM* (propaganda via e-mail não solicitado); Piadas, fotos e outros que não são pertinentes à empresa; Outros assuntos que não são pertinentes à empresa;

* Ou outros conforme exemplos demonstrados na Política de Utilização de Rede da empresa.