Conteúdo

Informações sobre o Documento	
Modelo	Política de Segurança da Informação
Versão atual	3.0

Revisões e Aprovações		
Responsável por	**Nome**	**Data de Execução**
Revisão/Aprovação		<dd-mm-aaaa>
Divulgação		<dd-mm-aaaa>

Histórico de Versões			
Versão	**Data**	**Responsável**	**Descrição da Alteração**
1.0	15/03/2010	Depto de TI – Setor de Segurança e Auditoria	Criação do documento
2.0	09/06/2010	Depto. De Comunicação e Marketing Institucional	Alteração de layout e numeração de páginas
3.0	11/10/2011	Depto. Jurídico e Depto. De Gestão de Pessoas	Inclusão da referência à legislação Inclusão de penalidades

BASEADO NA NORMA ABNT:ISO 17799:2005 (21:204.01-010)

A Política de segurança da informação, na EMPRESA, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento da EMPRESA, ou acesso a informações pertencentes à EMPRESA. Todo e qualquer usuário de recursos computadorizados da EMPRESA tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática. A violação desta política de segurança é qualquer ato que:

1. *Exponha a EMPRESA a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.*
2. *Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.*
3. *Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.*

1. OBJETIVOS DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da EMPRESA.

2. MISSÃO DA ÁREA DE TECNOLOGIA DA INFORMAÇÃO

Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade da informação necessária para a realização do negócio da EMPRESA. Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

4. RESPONSABILIDADE PELA INFORMAÇÃO

É DEVER DE TODOS NA EMPRESA considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a EMPRESA e deve sempre ser tratada profissionalmente.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade do Gerente/Supervisor de cada área estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

1 – Pública

2 – Interna

3 – Confidencial

4 – Restrita

Conceitos:

Informação Pública: É toda informação que pode ser acessada por usuários da organização, clientes , fornecedores, prestadores de serviços e público em geral.

Informação Interna: É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.

Informação Confidencial: É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.

Informação Restrita: É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Todo Gerente/Supervisor deve orientar seus subordinados a não circularem informações e/ou mídias consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente o conceito "mesa limpa", ou seja, ao terminar o trabalho não deixar nenhum relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

6. DADOS DOS FUNCIONÁRIOS

A EMPRESA se compromete em não acumular ou manter intencionalmente Dados Pessoais de Funcionários além daqueles relevantes na condução do seu negócio. Todos os Dados Pessoais de Funcionários que porventura sejam armazenados serão considerados dados confidenciais. Dados Pessoais de Funcionários sob a responsabilidade da EMPRESA não serão usados para fins diferentes daqueles para os quais foram coletados.

Dados Pessoais de Funcionários não serão transferidos para terceiros, exceto quando exigido pelo nosso negócio, e desde que tais terceiros mantenham a confidencialidade dos referidos dados, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários da EMPRESA. Por outro lado, os funcionários se comprometem a não armazenar dados pessoais nas instalações da EMPRESA, sem prévia e expressa autorização por parte da diretoria.

Mesmo que seja autorizado o armazenamento destes dados, EMPRESA não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança. Tais dados jamais poderão ser armazenados nos diretórios dos Servidores de empresa, e jamais poderão fazer parte da rotina de backup da EMPRESA.

7. ADMISSÃO E DEMISSÃO DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

O setor de Recrutamento e Seleção de Pessoal da EMPRESA deverá informar ao setor de Informática, toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou excluídos no sistema da EMPRESA. Isto inclui o fornecimento de sua senha ("password") e registro do seu nome como usuário no sistema (user-id), pelo setor de Informática.

Cabe ao setor solicitante da contratação a comunicação ao setor de Informática sobre as rotinas a que o novo contratado terá direito de acesso. No caso de temporários e/ou estagiários deverá também ser informado o tempo em que o mesmo prestará serviço á EMPRESA, para que na data de seu desligamento possam também ser encerradas as atividades relacionadas ao direito de seu acesso ao sistema.No caso de demissão, o setor de Recursos Humanos deverá comunicar o fato o mais rapidamente possível à Informática, para que o funcionário demitido seja excluído do sistema.

Cabe ao setor de Recursos Humanos dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da EMPRESA.Nenhum funcionário, estagiário ou temporário, poderá ser contratado, sem ter expressamente concordado com esta política.

8. TRANSFERÊNCIA DE FUNCIONÁRIOS / TEMPORÁRIOS / ESTAGIÁRIOS

Quando um funcionário for promovido ou transferido de seção ou gerência, o setor de cargos e salários deverá comunicar o fato ao Setor de Informática, para que sejam feitas as adequações necessárias para o acesso do referido funcionário ao sistema informatizado da EMPRESA.

9. PROGRAMAS ILEGAIS

A EMPRESA respeita os direitos autorais dos programas que usa e reconhece que deve pagar o justo valor por eles, não recomendando o uso de programas não licenciados nos computadores da EMPRESA. É terminantemente proibido o uso de programas ilegais (Sem licenciamento) na EMPRESA.

Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da EMPRESA, mesmo porque somente o pessoal da área de Ti tem autorização para instalação de programas previamente autorizados dentro da política de segurança da EMPRESA. Periodicamente, o Setor de Informática fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, estes deverão ser removidos dos computadores.

Aqueles que instalarem em seus computadores de trabalho tais programas não autorizados, se responsabilizam perante a EMPRESA por quaisquer problemas ou prejuízos causados oriundos desta ação, estado sujeitos as sansões previstas neste documento.

10. PERMISSÕES E SENHAS

Todo usuário que acessar os dados da rede da EMPRESA deverá possuir um *login* e senha previamente cadastrados pelo pessoal de TI.

Quem deve fornecer os dados referente aos direitos do usuário é o responsável direto pela sua chefia, que deve preencher uma ficha e entregá-la ao departamento de RH. Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas ou equipamentos de informática da EMPRESA, o setor de origem do novo usuário deverá comunicar esta necessidade ao setor de TI, por meio de memorando ou e-mail, informando a que tipo de rotinas e programas o novo usuário terá direito de acesso e quais serão restritos.

A área de TI fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 45 (quarenta e cinco) dias. Por segurança, a área de TI recomenda que as senhas tenham sempre um critério mínimo de segurança para que não sejam facilmente copiadas, e não possam ser repetidas.

Todos os usuários responsáveis pela aprovação eletrônica de documentos (exemplo: pedidos de compra, solicitações e etc.) deverão comunicar ao Setor de TI qual será o seu substituto quando de sua ausência da EMPRESA, para que as permissões possam ser alteradas (delegação de poderes). Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso devera ser bloqueada tão logo este tenha terminado o seu trabalho e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo pessoal de TI.

11. COMPARTILHAMENTO DE DADOS

Não é permitido o compartilhamento de pastas nos computadores e desktops da EMPRESA. Todos os dados deverão ser armazenados nos Servidores da rede, e a autorização para acessá-los deverá ser fornecida pelo Servidor AD (Active Directory). O Pessoal de TI está orientado a periodicamente todos os compartilhamentos existentes nas estações de trabalho e garantir que dados considerados confidenciais e/ou restritos não estejam armazenados na rede.

Os compartilhamentos de impressoras devem estar sujeitos as autorizações de acesso do AD. Não são permitidos na EMPRESA o compartilhamento de dispositivos móveis tais como *pen drivers,* discos externos/removíveis e outros.

12. BACKUP (CÓPIA DE SEGURANÇA DOS DADOS)

Todos os dados da EMPRESA deverão ser protegidos através de rotinas sistemáticas de Backup. Cópias de segurança do sistema integrado e servidores de rede são de responsabilidade do Setor Interno de TI e deverão ser feitas diariamente. Ao final de cada mês também deverá ser feita uma cópia de segurança com os dados de fechamento do mês, do Sistema Integrado.

Esta cópia será feita imediatamente após a comunicação formal da Contabilidade, por meio de memorando, que o referido mês foi encerrado. Nos meses pares, a Informática enviará 01 (uma) cópia extra da fita do "backup" de fechamento do referido mês, para ser arquivada na Contabilidade.

As copias deverão ser feitas em mídias removíveis e deverão abranger todos os dados da EMPRESA, que deverão estar nos servidores. As copias deverão ser protegidas por senhas para evitar que pessoas não autorizadas tenham acesso a estes dados em caso de perda ou roubo da mídia.

As Copias deverão ser feitas de forma escalonada em Midas diferentes para cada dia da semana. As mídias deverão ser armazenadas em local seguro, fora das instalações do CPD para evitar perda de dados em casos sinistros. Semanalmente, no final do expediente de sexta feira

um conjunto de backup devera ser enviado para um local externo em outro endereço a ser definido pela diretoria. Neste local devera haver permanentemente um conjunto completo de backup capaz de restaurar todos os dados da EMPRESA em caso de sinistro.

O conjunto de backup armazenado externamente deverá sofrer rodízio semanal com um dos conjuntos de backup ativo. Validação do Backup – Mensalmente o backup devera ser testado pelo pessoal de Ti, voltando-se parte ou todo o conteúdo do backup em um HD previamente definido para este fim . Esta operação devera ser acompanhada pelo Gerente da EMPRESA responsável por supervisionar a área de Ti.

13. CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

Não é política da EMPRESA o armazenamento de dados em desktops individuais, entretanto, existem alguns programas fiscais que não permitem o armazenamento em rede. Nestes e em outros casos, o pessoal de TI deverá alertar ao usuário que ele deve fazer backup dos dados de sua maquina periodicamente.

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da EMPRESA.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da EMPRESA o Setor de Informática disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações. Estas informações serão incluídas na rotina diária de backup da Informática.

14. SEGURANÇA E INTEGRIDADE DOS DADOS

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de TI, assim como a manutenção, alteração e atualização de equipamentos e programas.

15. PROPRIEDADE INTELECTUAL E DIREITOS AUTORAIS

São de propriedade da EMPRESA todos os programas, imagens, vídeos, sons, documentos, *designs*, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a EMPRESA, conforme estabelecido na legislação vigente (LEI FEDERAL Nº 9.609 , DE 19 DE FEVEREIRO DE 1998 e LEI FEDERAL Nº 9.610, DE 19 DE FEVEREIRO DE 1998..

16. ACESSO À INTERNET

O acesso à Internet será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na EMPRESA. Sites que não contenham

informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados. O uso da Internet será monitorado pelo Setor de Informática, inclusive através de "logs" (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) da Internet é atribuição da Direção da EMPRESA, com base em recomendação do Supervisor de Informática. Não é permitido instalar programas provenientes da Internet nos microcomputadores da EMPRESA, sem expressa anuência do setor de Informática, exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (*downloads*), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;

- De conteúdo pornográfico ou relacionados a sexo;

- Que defendam atividades ilegais;

- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;

- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios da EMPRESA;

- Que promovam discussão pública sobre os negócios da EMPRESA, a menos que autorizado pela Diretoria;

- Que possibilitem a distribuição de informações de nível "Confidencial".

- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

17. USO DO CORREIO ELETRÔNICO (E-MAIL)

O correio eletrônico fornecido pela EMPRESA é um instrumento de comunicação interna e externa para a realização do negócio da EMPRESA. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da EMPRESA, não podem ser contrárias à legislação vigente e nem aos princípios éticos da EMPRESA.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;

- Possam trazer prejuízos a outras pessoas;

- Sejam hostis e inúteis;

- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

- Possam prejudicar a imagem da organização;

- Possam prejudicar a imagem de outras empresas;

- Sejam incoerentes com as práticas e políticas formais da EMPRESA.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de Informática, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no Sistema de correio eletrônico o Setor de Informática fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites da web), nos computadores da EMPRESA. O Setor de Informática poderá, visando evitar a entrada de vírus na EMPRESA, bloquear o recebimento de e-mails provenientes de sites gratuitos.

18. NECESSIDADE DE NOVOS SISTEMAS, APLICATIVOS E EQUIPAMENTOS

O Setor de Informática é responsável pela aplicação da Política da EMPRESA em relação a definição de compra e substituição de “software” e “hardware”. Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo setor de Informática. Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

19. USO DE LAPTOPS, NOTEBOOKS, TABLETS E SMART PHONES NA EMPRESA

Os usuários que tiverem direito ao uso de computadores pessoais ou qualquer outro equipamento computacional pessoal e/ou móvel (laptop, notebook, tablet, smart phone), de propriedade da EMPRESA, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários têm como objetivo a realização de atividades profissionais.

- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

- O usuário não deve alterar a configuração do equipamento recebido. Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;

- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.

- Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível;

- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;

- Comunique ao seu superior imediato e ao Setor de Informática;

- Envie uma cópia da ocorrência para o Setor de Informática.

20. RESPONSABILIADE DOS GERENTES / SUPERVISORES

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos sistemas e informações da EMPRESA, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de Informática fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;

- Quem está autorizado a acessar determinada rotina e/ou informação;

- Quem acessou determinada rotina e informação;

- Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

- Que informação ou rotina determinado usuário acessou;

- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

21. SISTEMAS DE TELECOMUNICAÇÕES

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da EMPRESA, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do setor de Informática, de acordo com as definições da Diretoria da EMPRESA. Ao final de cada mês, para controle, serão enviados relatórios informando a cada gerência quanto foi gasto por cada ramal.

22. USO DE ANTIVÍRUS

Todo arquivo em mídia proveniente de entidade externa a EMPRESA deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo setor de Informática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

23. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações, independentes de outras providências legais aplicáveis:

1 Advertência verbal;
2 Advertência formal;
3 Suspensão;
4 Rescisão do contrato de trabalho;
5 Outras ações disciplinares e/ou processo civil ou criminal.