POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ambipar GROUP

I. APRESENTAÇÃO

A A Ambipar atua em diversos segmentos para oferecer serviços e produtos completos voltados à gestão ambiental. Em franca expansão mundial, a Ambipar respeita as regras de compliance e responsabilidade socioambiental, prezando a ética e o pronto atendimento às demandas de seus clientes.

Sendo assim a política de segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Ambipar para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários.

Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida internacionalmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

1. OBJETIVO

Este documento tem como objetivo garantir a confidencialidade, integridade, disponibilidade, legalidade, autenticidade e auditabilidade das informações da organização e de todos aqueles que fazem parte dela, tais como clientes, fornecedores, colaboradores e acionistas.

2. CAMPO DE APLICAÇÃO

Aplica-se a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam a Ambipar ou a suas subsidiárias.

Todo e qualquer usuário de recursos computacionais da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

3. CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- Confidencialidade: Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- Disponibilidade: Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;
- Integridade: Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

4. DEFINIÇÕES

Informação: resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema.

Ativos de Informação: conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.

Sistemas de informação: de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.

Segregação de funções: consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.

Gestor da Tecnologia da Informação: Área de TI da Ambipar com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela empresa.

5. CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida no desenvolvimento das atividades da empresa deve ser classificada de acordo com os níveis de confidencialidade abaixo:

1. Pública: É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral. Por exemplo: informações disponíveis na página da Internet da Ambipar.

2. 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. Exemplo: Comunicado RH direcionados aos colaboradores.

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

4. 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. Exemplo: dados da folha de pagamento são de acesso restrito apenas ao setor de RH.

6. RESPONSABILIDADES

De forma geral, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

- Cumprir fielmente a Política de Segurança da Informação da Ambipar;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela Ambipar;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Ambipar;

- Não utilizar os recursos tecnológicos da Ambipar em redes públicas, sem os devidos protocolos de segurança (exemplo: Rede sem fio publica de aeroportos, cafeterias, etc.);
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de Tecnologia da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

É dever de todos dentro da Ambipar:

Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a Ambipar e deve sempre ser tratada profissionalmente.

É de responsabilidade do Diretor/Superintendente/ Gerente/Coordenador/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

São boas práticas:

Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;

Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

II. DIRETRIZES GERAIS

1. Dados Pessoais de Funcionários

A Ambipar 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 serão considerados confidenciais.

Os dados pessoais de funcionários sob a responsabilidade da Ambipar 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.

2. Admissão/demissão de colaboradores

O setor de RH da Ambipar deverá informar ao Gestor da Tecnologia da Informação de toda e qualquer movimentação de colaboradores, temporários e/ou estagiários, e admissão/demissão de funcionários, para que os mesmos possam ser cadastrados ou

descadastrados nos sistemas da empresa. O RH deverá questionar ao setor responsável pela contratação quais sistemas e repositórios de arquivos de trabalho o novo colaborador deverá ter direito de acesso.

Essas informações deverão ser registradas e encaminhadas para o Gestor da Tecnologia da Informação através do "RH.003 – Concessão / Revogação de Acessos", o Gestor da Tecnologia da Informação da Ambipar fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo usuário no seu primeiro acesso.

No caso de desligamento, o setor de RH deverá comunicar o fato na mesma data ao Gestor da Tecnologia da Informação, por meio do "RH.003 – Concessão / Revogação de Acessos" para que todos os acessos concedidos sejam revogados.

Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação da Ambipar.

3. Política de senhas

As senhas de acesso dos sistemas utilizados pela empresa/na empresa, fornecidas pelo Gestor da Tecnologia da Informação da Ambipar, são de uso pessoal e intrasferível, sendo EXPRESSAMENTE vedado o compartilhamento com outro usuário, caracterizando falta contratual gravíssima.

O acesso e os dados/atividades gerados através do login e senha fornecidos pelo Gestor da Tecnologia da Informação da Ambipar são de responsabilidade do usuário.

As senhas configuradas para todos os acessos devem atender aos seguintes requisitos de complexidade recomendados para serem aceitas pelas políticas sistêmicas:

- As senhas não podem conter o nome da conta do usuário, o nome do usuário ou parte dele;
- As senhas devem conter caracteres de três das seguintes categorias: - Letras maiúsculas - Letras minúsculas - Dígitos base 10 (0 a 9) - Caracteres não alfanuméricos (caracteres especiais): (~!@#$%^&*- +='|\() {} []:;'" <>,.? /);
- As senhas expiram a cada 90 dias, sendo obrigatória a troca no fim deste período, seguindo os requisitos informados acima e não devendo se repetir as senhas definidas nas últimas 5 senhas;
- As senhas iniciais devem ser aleatórias conforme recomendação de boas práticas, não seguindo padrões que possam facilmente ser descobertos ou aplicando a mesma senha padrão para todos os usuários criados, o que colocaria em risco a segurança dos usuários da Ambipar.
- As senhas iniciais de usuários do domínio devem ser trocadas logo no primeiro acesso a rede da Ambipar. Caso o equipamento esteja fora do domínio da empresa, a troca deverá ser realizada via VPN. Para demais sistemas, efetuar a troca normalmente no próprio sistema.

Sempre que um usuário é desligado da organização, todas as suas senhas e acessos são revogados no mesmo dia.

4. Arquivos de Trabalho

Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do negócio, são mantidos nos servidores de arquivos da Ambipar.

São exemplos de arquivos de trabalho:

- Planilha de faturamento;
- Notas fiscais;
- Propostas comerciais;
- Relatórios de análise técnica;
- Planilhas de medição;
- Documentação de sistema utilizada como insumo para o trabalho de análise e medição.

O acesso ao servidor de arquivo fora das dependências da Ambipar é bloqueado e proibido, salvo se realizado através de VPN, com a devida permissão do Gestor da Tecnologia da Informação.

5. Arquivos Individuais

São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para clientes. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas. A cópia de segurança destes arquivos é de responsabilidade dos próprios usuários.

Não é permitido aos usuários o uso ou armazenamento dos tipos de arquivos abaixo relacionados em suas estações de trabalho:

- Programas não licenciados ou não homologados para uso na Ambipar;
- Músicas, filmes, séries, programas de TV;
- Vídeos não relacionados à atividade profissional;
- Conteúdo pornográfico ou relacionado a sexo.

Havendo necessidade de se realizar o compartilhamento de dados entre usuários (internos e/ou externos), deve-se utilizar o servidor de arquivo ou e-mail profissional fornecido pela Ambipar com consentimento do Gestor responsável.

6. Compartilhamento de Pasta e Dados

O compartilhamento de pastas e arquivos de trabalho cujo conteúdo seja classificado como sendo de informação CONFIDENCIAL ou RESTRITA é proibido através dos seguintes:

- Google Talk, WhatsApp, Viber ou qualquer outro comunicador de mensagens instantâneas;
- Compartilhamento de pastas do Windows;
- Bluetooth;
- Cópia via pen drive ou qualquer outro dispositivo removível;
- Google Drive, Dropbox, iCloud, OneDrive ou qualquer outro drive virtual.

7. Cópias de Segurança, Recuperação e Integridade dos Sistemas e de seus Bancos de Dados

Cópias de segurança dos sistemas, repositórios na rede de arquivos de trabalho, bancos de dados e configurações dos equipamentos e servidores de rede são de responsabilidade exclusiva do Gestor da Tecnologia da Informação.

8. Uso da Internet

O uso da Internet será monitorado pelo Gestor da Tecnologia da Informação, através do uso de sistema de registro de navegação que informa qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

A definição dos funcionários que terão permissão para uso (navegação) de sites restritos, como por exemplo, redes sociais, é atribuição da administração da empresa, a partir da solicitação de seu Diretor/Superintendente/ Gerente/Coordenador/Supervisor.

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:

- estações de rádio;
- De jogos on-line;
- 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 relacionados aos negócios da FATO, que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

Qualquer acesso às redes sociais que não seja relacionado com a área de interesse da empresa não é permitido e, sendo assim, passível de punição.

Em casos, onde seja necessário o acesso a determinado site ou porta bloqueados, deve ser aberto chamado "TI.002 – Infraestrutura (Suporte Nível 1 / Rede e Internet / Servidores)"

com a URL do site e/ou o número da porta, para que o Gestor da Tecnologia da Informação providencie a liberação junto ao firewall da Ambipar.

9. Uso do Correio Eletrônico ("e-mail")

O correio eletrônico fornecido pela Ambipar é um instrumento de comunicação interna e externa para a realização dos negócios da empresa.

As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da Ambipar, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos no "Código de Ética e Conduta".

O uso do correio eletrônico é uma ferramenta usada para enviar e receber mensagens de maneira instantânea através da Internet e o usuário é responsável por toda mensagem enviada pelo seu endereço.

Não é permitido o cadastro de contatos pessoais nos sistemas de mensagens instantâneas (ao utilizar a conta profissional @ambipar.com); e nem a utilização de contas pessoais.

É obrigatória a utilização da autenticação multifator da Microsoft, com a imposição de uso de senhas do aplicativo Microsoft Authenticator para o uso de aplicativos com o e-mail corporativo que não sejam navegadores. Para os navegadores, o usuário pode informar outros modos de autenticação, além da senha do aplicativo autenticador, como envio de SMS ou chamada telefônica para telefone de uso pessoal ou corporativo, uma vez que a senha de e-mail do usuário é de uso estritamente pessoal.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da Ambipar, suas subsidiárias e/ou de outras empresas;
- Sejam incoerentes com as políticas estabelecidas no "Código de Ética e Conduta" da Ambipar.
- Uso de e-mail gratuitos (Yahoo!, Hotmail, etc.), nos computadores da Ambipar.

Importante que os usuários se atentem ao abrir um e-mail de um remetente desconhecido, principalmente se este e-mail redirecionar a um link e/ou contiver qualquer tipo de anexo. Para maior segurança em caso de e-mail suspeito, o mesmo deverá ser encaminhado para spam@ambipar.com onde o Gestor da Tecnologia da Informação efetuará uma análise mais profunda e determinará o bloqueio ou a liberação do e-mail.

O Gestor da Tecnologia da Informação poderá, visando evitar a entrada de vírus ou qualquer outro malware nos computadores da Ambipar, bloquear o recebimento de e-mails provenientes de e-mails gratuitos.

10. Necessidade de Novos Sistemas, Aplicativos e/ou Equipamentos

O Gestor da Tecnologia da Informação é responsável pela definição de compra, substituição e instalação de todo e qualquer "software" e "hardware".

A aquisição de software e de hardware somente poderá ser feita via chamado no sistema Workflow ("TI.012 – Aquisição de Equipamentos Eletrônicos" para aquisição de equipamentos e licenças de software, ou "TI.002 – Infraestrutura (Suporte Nível 1 / Rede e Internet / Servidores)" para instalação de softwares já licenciados), com autorização anexada do diretor do usuário solicitante. Não é permitida a compra ou o desenvolvimento de "softwares" diretamente pelos usuários.

A entrega dos equipamentos só será realizada perante assinatura de termo de responsabilidade, direcionado ao colaborador responsável pelo equipamento, através de chamado no Workflow da categoria "TI.019 – Termo de responsabilidade de Equipamentos Eletrônicos".

11. Uso de Equipamentos de Propriedade da Empresa

É vedado o uso de equipamento pessoal (notebook/desktop) para exercício da função, fornecendo a Companhia equipamento compatível com as atividades executadas pelo colaborador/parceiro quando o caso, salvo autorização expressa da Alta Gestão, mediante requerimento formal pela parte.

A instalação de softwares e hardwares são de responsabilidade do Gestor da Tecnologia da Informação da Ambipar, respeitando-se os contratos e termos de manutenção, licenciamento e aquisição celebrados pela Ambipar.

Não é autorizado ao usuário instalar softwares, inclusive aqueles disponibilizados pela Internet (ainda que a título gratuito, como os do tipo freeware/shareware) ou novos componentes de hardware em equipamento da Ambipar, mesmo quando estes se destinem ou facilitem as atividades profissionais do usuário.

A manutenção dos equipamentos de infraestrutura é de responsabilidade do Gestor da Tecnologia da Informação. Fornecedores terceiros poderão realizar a manutenção apenas com autorização do Gestor da Tecnologia da Informação, e com orçamento pré-aprovado pela diretoria.

É dever do usuário permitir acesso ao seu equipamento pelos colaboradores autorizados do Gestor de Tecnologia da Informação, para realizar manutenção e inspeção (inclusive remota), em data e horário previamente combinados, incumbindo ao Gestor da Tecnologia da Informação, ainda, deletar eventuais arquivos, softwares ou hardwares instalados/salvos no equipamento em desatenção a presente Política, sem prévio aviso/consentimento.

Os usuários que estiverem de posse de qualquer equipamento (desktop, notebook, celular ou tablet ou outro equipamento de tecnologia da informação) de propriedade da Ambipar 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;
- O usuário não deve instalar ou remover nenhum programa do equipamento recebido. Também não deve alterar a configuração de nenhum programa previamente instalado.

A utilização de mídias removíveis (USB, cartões, CD, DVD), só podem ser utilizados com autorização prévia do gestor direto do usuário, e devem ser autorizados somente pelo Gestor da Tecnologia da Informação, mediante a expressa autorização citada.

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, ônibus, 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 ou roubo:

- Registre a ocorrência em uma delegacia de polícia;
- Comunique o fato o mais rápido possível ao seu superior imediato e ao Gestor da Tecnologia da Informação;
- Envie uma cópia do boletim de ocorrência para o RH.

12. Dados

Todos os dados (arquivos, documentos, apresentações etc.), obrigatoriamente, devem ficar armazenados no servidor de arquivos indicado pela Ambipar ("rede"), visando a proteção, manutenção e a confidencialidade destes dados, pois os dados armazenados localmente nos computadores não estão protegidos por backups periódicos, podendo, em caso de problemas no equipamento, ocorrer a perda parcial ou total de dados importantes para a Companhia.

A desatenção a tal diretiva pode caracterizar falta contratual, uma vez que vai contra as boas práticas de segurança da informação.

Somente dados pertinentes à empresa devem ser mantidos nos computadores da Ambipar.

É de responsabilidade do Gestor da Tecnologia da Informação, garantir a execução de rotinas de backup periódicos em todos os servidores da Ambipar, visando a prevenção da perda de dados.

13. Impressão

O usuário deve garantir que as impressões de documentos com conteúdo confidencial não sejam expostas a outros usuários da impressora compartilhada. Deve garantir ainda, o descarte correto de tais documentos.

Com o intuito de viabilizar a segurança da informação, as impressoras da Ambipar são dotadas, em sua maioria, de sistema que permite somente ao usuário obter as impressões, com o uso do pin ou por meio do crachá.

14. Sistema de Telecomunicações

O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos da Ambipar, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade do Gestor da Tecnologia da Informação, de acordo com as definições da administração da empresa.

15. Uso de antivírus

Todo arquivo obtido através da Internet ou recebido de entidade externa a Ambipar deve ser verificado por programa antivírus.

Todas as estações de trabalho possuem software antivírus instalado. A sua atualização será automática, agendada pelo Gestor da Tecnologia da Informação, via rede.

O usuário não pode, em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

III. RESPONSABILIDADES DOS DIRETORES/SUPERINTENDENTES/GERENTES /COORDENADORES/SUPERVISORES

Os diretores, superintendentes, gerentes, coordenadores e supervisores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da empresa, cabendo a eles verificarem se eles estão acessando exatamente os sistemas e as áreas de dados 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 Gestor da Tecnologia da Informação fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinado sistema e/ou informação;
- Quem acessou determinada sistema e informação;
- Quem autorizou o usuário a ter permissão de acesso à determinado sistema ou informação;
- Que informação ou sistema determinado usuário acessou;
- Quem tentou acessar qualquer sistema ou informação sem estar autorizado.

IV. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

É qualquer ato que:

- 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;
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos;
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

V. OUTROS

Qualquer outro assunto relacionado a TI e que não foi abordado neste documento deverá ser informado ao Gestor da Tecnologia da Informação para que orientações sejam dadas.

VI. PENALIDADES

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações:

- Advertência formal;
- Suspensão;
- Rescisão do contrato de trabalho;

Outra ação disciplinar e/ou processo civil ou criminal.

VII. VIGÊNCIA

O disposto no presente documento entrará em vigor na data de publicação do comunicado que o anunciar, sendo aprovada pelo Conselho de Administração.