Elaboração/Revisão			Aprovação		
Nome	Visto	Data	Nome	Visto	Data
Rafael Almeida		01/04/2022	Lilian Fernandes		01/04/2022

Sumário

ÚLTIMA REVISÃO		
Número	**Descrição**	**Data**
01	Revisão de política de senha (6.1.1), caminhos no servidor (6.2.1) e Telefonia (6.7), e adicionado item 6.3.4 ataque cibernético, conforme SAC 002/22	01/04/2022
00	Emissão Inicial.	05/04/2019

1. Objetivo

Estabelecer as regras básicas de uso dos recursos de tecnologia da informação fornecidos pela da Bras-mol.

2. Aplicação

Este documento aplica-se a todos os usuários de tecnologia da Bras-mol.

3. Apresentação

3.1 Missão

A segurança é um dos mais importantes dentre as preocupações de qualquer empresa. Nesse documento apresentaremos um conjunto de instruções e procedimentos para normatizar e melhorar nossa visão e atuação em segurança.

3.2 A Empresa e a Política de Segurança

Todas as normas aqui estabelecidas devem ser seguidas à risca por todos os colaboradores, parceiros e prestadores de serviços. Ao receber essa cópia da Política de Segurança da Informação, o/a sr/sra comprometeu-se a respeitar todos os tópicos aqui abordados e está ciente de que seus e-mails e navegação na internet / intranet podem estar sendo monitorados.
A equipe de T.I encontra-se a total disposição para saneamentos de dúvidas e auxílios técnicos.

3.3 Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada em regime de CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a Bras-Mol e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

3.4 Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no termo de aceite concedido pela Bras-Mol Molas e Estampados Ltda. A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção, ou ainda se o colaborador que o

recebeu a cópia deste não estiver cumprindo as condições definidas no aceite.

3.5 Gestores de Pessoas e /ou Processos

É de responsabilidade dos gestores:

- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão;
- Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da Bras-Mol Molas e Estampados Ltda.;
- Solicitar aos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Bras-Mol Molas e Estampados Ltda.;
- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI;
- Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

3.6 Área de Tecnologia da Informação

É de responsabilidade da área de tecnologia:

- Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.
- Segregar as funções administrativas, operacionais e administrativas a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Bras-Mol Molas e Estampados Ltda.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.
- Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo.Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:
    - Os usuários (logins) individuais de colaboradores serão de responsabilidade do próprio colaborador;
    - Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante;
    - Os usuários (logins) compartilhados serão de responsabilidade do gestor da área.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

4. O Não Cumprimento desta Política

O não cumprimento dessa política acarretara em sanções administrativas em primeira instancia, podendo acarretar no desligamento do Colaborador de acordo com a gravidade da ocorrência.

5. Autenticação

A autenticação nos sistemas de informática será baseada em um login e senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo. Infelizmente esse meio também não é o mais inseguro.

Senhas como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, brasil), datas (11092001) e outros são extremamente fáceis de descobrir. Então aprenda a criar senhas de forma coerente, observando nossa política de senhas.

6. Regras em Geral

6.1 Política de Senhas

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Bras-Mol e / ou terceiros. O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados na Bras-Mol, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Bras-Mol e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.
O Departamento de Recursos Humanos da Bras-Mol é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.
A equipe de T.I responde pela criação da identidade lógica dos colaboradores na instituição, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.
Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

6.1.1 Elaboração de Senhas:

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo), sempre que possível.
Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.
Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o Departamento e T.I.
Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).
Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 90 (Noventa) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios

administrativos devem exigir a troca de senhas a cada 60 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.
Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.
Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

6.1.2 Dica para Elaboração de Senha:

Uma senha deverá conter no mínimo 6 caracteres alfanuméricos (letras e números) com diferentes caixas.
Para facilitar a memorização das senhas, utilize padrões mnemônicos. Por exemplo:

- **eSus6C** (eu SEMPRE uso seis 6 CARACTERES);
- **odlamp0709** (ouviram do Ipiranga as margens plácidas 7 de setembro) ;
- **s3Nh45** (A palavra senha onde 3 substitui o E, o 4 o A e o 5 o S).

As senhas terão um tempo de vida útil determinado pela equipe de T.I, devendo o mesmo ser respeitado, caso contrário o usuário ficara sem acesso aos sistemas.

- Sua senha não deve ser jamais passada a pessoas de outros setores, o departamento de T.I somente solicitara a sua senha caso for realmente necessário. Caso desconfie que sua senha não esteja mais segura, sinta-se à vontade para altera-la, mesmo antes do prazo determinado.
- Tudo que for executado com sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.

6.2 Utilização da Rede

A função básica da Rede Local é permitir o compartilhamento de recursos e informações nos Servidores, possibilitando centralizar dados pertinentes às áreas, levando ao aumento da segurança, diminuição de redundância de informações e economia de recursos, além de garantir um melhor gerenciamento dos usuários de informática. Através deste gerenciamento, consegue-se:

- Impedir o acesso de usuários não autorizados às informações da Bras-Mol;
- Segmentar sistema, softwares e diretórios por usuário cadastrado, criando perfis de acesso;
- Garantir cópias (backup) gerais dos arquivos gravados no Servidor, de modo que os usuários tenham possibilidade de recuperação de arquivos e;
- Gravar todas as intervenções dos usuários, registrando nomes, datas, horários e endereços das estações e seus respectivos acessos.

Todas as dúvidas sobre a utilização dos recursos de informática devem ser levadas à Área de Tecnologia, através de ramais, telefones ou e-mail próprios, que possui condições técnicas para suporte adequado aos usuários. É de suma importância que os usuários observem alguns aspectos que colaboram para a boa utilização e, principalmente, segurança do ambiente de Rede:

6.2.1 Diretórios específicos da Rede:

Além do diretório pessoal, os usuários têm acesso aos seguintes diretórios de trabalho da rede: \\servidor\Público, que é um diretório compartilhado a todos os usuários, possibilitando a troca de arquivos e o trabalho colaborativo esta pasta é de livre acesso a todos os usuários, a pasta \\servidor\arqbrasmol \ “Departamentos cada departamento tem uma pasta criada no ambiente de rede elas são restritas aos usuários de cada departamento.

Excepcionalmente, podem existir casos de usuários que de forma justificada necessitem de acesso a outros compartilhamentos e / ou áreas. Neste caso a solicitação do acesso deverá ser formalizada pela gerência da área.

6.2.2 Gravação de Arquivos:

Todos os usuários possuirão uma área em rede de tamanho determinado, com acesso individual e não compartilhado, e acesso ao diretório comum da área em que trabalha.

Os arquivos de trabalho deverão ser gravados em diretórios próprios e adequados da Rede (diretório pessoal nominal ou diretório de sua área relacionado ao assunto), utilizando-se de terminologia que facilite a localização e identificação com o seu conteúdo.

- Não deverão ser utilizados para os arquivos nomes constrangedores, que não condizem com a imagem e seriedade da Bras-Mol;
- Não deverão ser atribuídos aos nomes dos arquivos: acentos, espaços em branco, cedilha (Ç) e outros caracteres especiais que possam vir a causar incompatibilidade com outros aplicativos, evitando-se, também, nomes de arquivos longos (mais que 8 caracteres);
- Os nomes dos arquivos nunca deverão iniciar com “~” ou utilizar a extensão (tipo de

arquivo) como".tmp" pois rotinas dos servidores eventualmente poderão apagar os arquivos.

6.2.3 Exemplo de Gravação Adequada na Rede:

Usuário João, pertencente ao Departamento de Projetos, deverá gravar seus arquivos:

- No diretório \\servidor\arqbrasmol \Projetos os arquivos pertencentes à área, possibilitando o compartilhamento pelos outros usuários de sua área.

Todos os arquivos não necessários às atividades devem ser eliminados da Rede, de modo a colaborar com o desempenho do ambiente. Nos casos especiais de armazenamento de arquivos por necessidade esporádica ou prazo legal, tal procedimento deve ser comunicado a Área de tecnologia, que manterá tais arquivos em diretórios ou mídias próprias, de modo a não impactar o espaço e desempenho do ambiente de rede.

6.3 Política de E-mail

O objetivo desta norma é informar aos colaboradores quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico é para fins corporativos e relacionados às atividades do colaborador / usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Bras-Mol e também não cause impacto no tráfego da rede.

6.3.1 Cuidados a serem tomados:

- "Não abra anexos com as extensões:".bat, .exe, .src, .link e .com" se não tiver certeza de que solicitou esse e-mail.
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc.;
- Não reenvie e-mails do tipo corrente, aviso de vírus, aviso da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.;
- Não mande e-mails para mais de 10 pessoas de uma única vez.;
- Evite anexos muito grandes.

6.3.2 Acrescentamos que é Proibido aos Colaboradores o Uso do Correio Eletrônico:

- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Bras-Mol

vulneráveis a ações civis ou criminais;

- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer a Bras-Mol estiver sujeita a algum tipo de investigação.

6.3.3 Produzir, Transmitir ou Divulgar Mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie aos interesses da Bras-Mol;
- Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer Pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior (es) a 15 MB para envio (interno e externo) e 15 MB para recebimento.
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Nota: As mensagens de Correio Eletrônico Sempre Deverão Incluir Assinatura com o seguinte formato:

- Nome do colaborador;
- Gerência ou departamento;
- Nome da empresa;
- Telefone(s);
- Correio eletrônico.

6.3.4 Ataques Cibernéticos

O sistema de monitoramento (Firewall PFSense) realiza o monitoramento e o bloqueio de possíveis ataques cibernéticos em nossa rede, porém é necessário ter cautela com os acessos a sites de downloads de torrents e demais aplicações seguir conforme itens. 6.4 e 8 desta PSI.

6.4 Política de Acesso a Internet

Todas as regras atuais da Bras-Mol visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Bras-Mol, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privados da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A Bras-Mol, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades

competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Como é do interesse da Bras-Mol que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Bras-Mol para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais. É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.
Os colaboradores com acesso à internet poderão fazer o download (baixar) somente de programas ligados diretamente às suas atividades de trabalho e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela área competente.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela equipe de T.I.
Os colaboradores não poderão em hipótese alguma utilizar os recursos da Bras-Mol para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado a Bras-Mol ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos da Bras-Mol para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estarão bloqueados e monitorados.

É proibido o uso de comunicador Instantâneos (WhatsApp, Skype, etc) não homologados/Autorizados pela equipe de T.I.
Lembrando novamente que o uso da internet estará sendo auditado constantemente e o usuário poderá vir a prestar contas de seu uso.

6.5 Política de Estações de Trabalho

Os equipamentos disponíveis aos colaboradores são de propriedade da Bras-Mol , cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da equipe de T.I, ou de quem este determinar.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante o notificação por e-mail para o técnico responsável.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Bras-Mol (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.
Os colaboradores da Bras-Mol e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da equipe de T.I.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe de T.I ou por terceiros devidamente contratados para o serviço.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pela Bras-Mol , seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custo diante de informações.
- Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador quando não estiverem sendo utilizados.

- Todos os recursos tecnológicos adquiridos pela Bras-Mol devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Bras-mol.

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

Cada estação de trabalho tem códigos internos que permitem que ela seja identificada na rede, e cada indivíduo possui sua própria estação de trabalho. Isso significa que tudo que venha a ser executado de sua estação acarretara em responsabilidade sua. Por isso sempre que sair da frente de sua estação, tenha certeza que efetuou o logoff ou travou a tela.

- Não instale nenhum tipo de software / hardware sem autorização da equipe de T.I;
- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria;
- Mantenha na sua estação somente o que for supérfluo ou pessoal. Todos os dados relativos à empresa devem ser mantido no servidor, onde existe um sistema de backup diário e confiável.

Caso não saiba como fazer isso, entre em contato com a equipe de T.I.

6.6 Impressoras

A Bras-Mol possui algumas políticas de impressão que devem ser seguidas, conforme instruções abaixo.

- É proibida a impressão de qualquer documento que não tenha relação com o trabalho na empresa.
- Todas as impressões e o seu conteúdo serão identificados por usuário, horário e local de impressão pela área de Tecnologia da Informação.
- As impressões por usuário serão auditadas mensalmente. O descumprimento desta política, identificado através do processo de auditoria, será apresentado mensalmente ao usuário e ao gerente e/ou diretor.

Orientações de Uso:

- Antes de imprimir, avalie se este procedimento é mesmo necessário. Muitos documentos podem ser arquivados e lidos em meio eletrônico;
- Ao tentar imprimir um mesmo documento pela segunda vez, verifique na impressora ou no balcão, se o documento não foi mesmo impresso;
- Se a impressão estiver errada e o papel puder ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão, com a face limpa para baixo. Se o papel servir para rascunho, deixe-o no gaveteiro ou leve-o para sua mesa;
- Se o papel não servir para mais nada, jogue-o no lixo;
- Se impressora emitir alguma folha em branco, recoloque-a na bandeja de impressão;
- Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastecê-la. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão;
- Imprima em frente e verso, sempre que possível. A impressora do já está configurada para isto;

6.7 Telefonia

Todas as facilidades da nossa central telefônica encontram-se documentadas IO053, o documento encontra-se disponível na pasta “\\servidor\arqbrasmol\publico\001 - Comunicado Interno”:

6.8 Dispositivos Moveis

A Bras-Mol deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis, para fins de trabalho.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua equipe de T.I, como: notebooks, smartphones e pen-drives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.
A Bras-Mol, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.
O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Bras-Mol , mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não carregá-los juntos.
O suporte técnico aos dispositivos móveis de propriedade da Bras-Mol e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.
Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.
Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da área responsável. O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da equipe de T.I.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Bras-Mol , notificar imediatamente seu gestor direto e departamento de Tecnologia. Também

deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Bras-Mol e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede da Bras-Mol deverá submeter previamente tais equipamentos ao processo de autorização da área responsável.

Equipamentos portáteis, como smart phones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

6.9 Data Center (CPD)

O acesso ao Datacenter somente deverá ser feito por pessoas devidamente autorizadas, todo acesso ao Datacenter, deverá ser registrado (usuário, data e hora).

Deverá ser executada semanalmente uma auditoria nos acessos ao Datacenter por meio do relatório de registro.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Nas localidades em que não existam colaboradores da área de tecnologia da informação, pessoas de outros departamentos deverão ser autorizadas para que possam ter acesso para exercer as atividades operacionais dentro do Datacenter, como: reparo de ar-condicionado, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado, que deverá preencher a solicitação de acesso prevista no Procedimento de Controle de Acesso ao Datacenter, bem como assinar o Termo de Responsabilidade.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização

com antecedência a qualquer colaborador responsável pela administração de liberação de acesso, conforme lista salva em Procedimento de Controle de Acesso ao Datacenter.

Deverão existir duas cópias de chaves da porta do Datacenter. Uma das cópias ficará de posse do coordenador responsável pelo Datacenter, a outra, de posse do coordenador de infraestrutura.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo colaborador solicitante e a autorização formal desse instrumento pelo responsável do Datacenter, de acordo com os termos do Procedimento de Controle e Transferência de Equipamentos.

6.10 Backup

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup” – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como HD, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

7. POLÍTICA SOCIAL

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando descoremos sobre segurança, isso é uma desvantagem. Por isso observe os seguintes tópicos:

- Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos.
- Não diga sua senha para ninguém. Nossa equipe técnica somente pedira sua senha caso seja extremamente necessário.
- Não digite suas senhas ou usuários em maquinas fora da rede Bras-Mol , especialmente fora da empresa.
- Relate a equipe técnica os pedidos externos ou internos que venham a discordar dos tópicos anteriores.

8. VÍRUS E CÓDIGOS MALICIOSOS

Mantenha seu antivírus atualizado. Provavelmente nossa equipe técnica irá se encarregar disso, mas caso não tenha sido feito ou você perceba que a atualização não está funcional, entre em contato com a mesma para que a situação possa ser corrigida. O uso de Pen drive ou CDs de fora da empresa deverá ser comunicado ao departamento de tecnologia antes de seu uso, a equipe realizara uma verificação antes de ser liberado para uso no computador.

Reporte atitudes suspeitas em seu computador à equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.

Suspeite de softwares que “Você clica e não acontece nada”.

9. CONTINUIDADE DO NEGÓCIO

De nada adianta uma informação segura se a mesma estiver indisponível para quem necessita dela. Por isso nossa equipe técnica conta com a sua com a sua colaboração para manter nossa empresa como líder de mercado. Entre em contato conosco sempre que julgar necessário.

10. MEMBROS DA EQUIPE DE TI

Nome	E-mail	Ramal	Celular / WhatsApp
Rafael Almeida	rafael.almeida@brasmol.com.br	-----	(11) 94950-2286

ANEXO 1. TERMO DE RECEBIMENTO E COMPROMISSO

Declaro que recebi uma cópia do **PSI - Política de Segurança da Informação** da Bras-Mol e estou ciente do seu conteúdo e da sua importância para o exercício de todas as atividades da empresa.

A assinatura do presente termo, anexo ao referido PSI, é a manifestação de minha livre concordância e do meu compromisso em cumpri-lo integralmente.

_____, _____, _____, _____.
(local) (dia) (mês) (ano)

Empresa:
_____

Nome:
_____

Cargo:
_____

Assinatura:
_____