Manual da Política de Segurança da Informação

Elaboração: Sistemas e Tecnologia

Aprovação: Sistemas e Tecnologia/Diretoria

Versão: 9

Código: M024

Vigente Desde: 10/2012

Última Versão: 09/2022

ÍNDICE

1. OBJETIVO

Este documento estabelece as regras e os controles sobre o uso de recursos de tecnologia para preservar a integridade, confidencialidade e disponibilidade das informações do Grupo BR Partners.

2. APLICABILIDADE

Os dispositivos deste documento são aplicáveis a todas as empresas do Grupo BR Partners, colaboradores, parceiros de negócios, fornecedores e prestadores de serviços, que atuem nos ambientes físicos e/ou tecnológicos para processar dados sensíveis controlados e/ou pertencentes ao Grupo BR Partners.

3. RESPONSABILIDADES

3.1. Tecnologia da Informação

A área de Tecnologia é responsável por:

- Garantir a segurança da informação nos recursos utilizados pelos colaboradores;
- Analisar as contratações dos serviços de informática providenciando uma análise de custo/benefício;
- Validar e homologar todos os programas e equipamentos utilizados no Grupo BR Partners;
- Efetuar bloqueios de acesso a arquivos, domínios e serviços de Internet que comprometam o uso de banda, a segurança do Grupo BR Partners ou o bom andamento dos trabalhos;
- Avaliar a necessidade de aquisição de softwares, bem como a sua compatibilidade;
- Proceder à instalação dos *softwares* adquiridos pelo Grupo BR Partners;
- Efetuar a transferência de *software* entre áreas ou entre computadores da mesma área;
- Prover suporte a todos colaboradores no tocante a infraestrutura operacional que garantam aos mesmos o bom desenvolvimento das suas atividades;
- Manter a disponibilidade da infraestrutura e redes garantindo a sustentação da Equipe de Negócios;
- Direcionar fornecedores de Tecnologia a seguirem boas práticas de Segurança da Informação referente a Sistemas de Tecnologia implantados;
- Viabilizar e testar novas tecnologias que possam trazer melhorias para os sistemas e ferramentas utilizadas pelo colaborador;
- Manter em local apropriado e em segurança os discos originais e seus *backups* (cópias de segurança), bem como os respectivos manuais e contratos de cessão de uso; e
- Acompanhar, juntamente com o usuário, o prestador de serviço, quando de atualizações de *software*/*hardware*, apresentações de novos aplicativos etc.

3.2. Sistemas

A área de Sistemas é responsável por:

- Suportar os sistemas utilizados pelo Grupo BR Partners;
- Aplicar as melhores práticas ITIL (*Information Technology Infrastruture Library*) no que tange a mudanças, incidentes, problemas e solicitações de sistemas;
- Mudanças: Abrange alterações e implantações de sistemas cumprindo os requisitos ITIL que envolve aprovação e homologação dos usuários de negócios além de gerenciamento de riscos e prioridades;
- Incidentes: Atendimento a qualquer chamado dos usuários: *bugs*, mau funcionamento, podendo através de incidentes também incluir, excluir ou alterar os acessos aos sistemas;
- Problemas: Quando um incidente se torna reincidente e é resolvido de forma paliativa é registrado o problema, onde a área de Sistemas junto com os fornecedores (caso aplicável) discute para dar uma solução definitiva;
- Solicitações/Demandas: Melhorias levantadas por colaboradores ou por fornecedores que são registradas para serem analisadas, debatidas e trabalhadas para serem implantadas posteriormente através de mudanças no ambiente de Produção. As demandas também controlam as aprovações das segregações de funções, geradas pela área de Sistemas e aprovadas pela área de *Compliance*.
- Monitorar as integrações dos Sistemas;
- Desenvolver ferramentas internas; e
- Analisar as contratações de novos sistemas providenciando uma análise de custo/benefício junto às áreas de negócio.

3.3. Colaboradores

Os colaboradores são responsáveis por:

- Proteger seus acessos aos sistemas (*login* e senha), tratando-os de forma confidencial e exclusiva, sendo de sua inteira responsabilidade qualquer consequência da utilização indevida;
- Cuidar dos equipamentos sob custódia e desligá-los ao final do expediente; e
- Respeitar os direitos autorais, regras de licenciamento de *softwares*, direitos de propriedade, privacidade e proteção de propriedade intelectual.

3.4. *Compliance*

A área de *Compliance* é responsável por:

- Monitorar e inspecionar as mensagens trocadas nos sistemas internos de comunicação; e

- Verificar possíveis restrições ao uso equipamentos, *softwares* e/ou liberação de acessos aos sistemas.

4. DESCRIÇÃO DA NORMA

4.1. Considerações Gerais

A informação é um ativo essencial para os negócios da organização e consequentemente necessita ser adequadamente protegida. As diretrizes da Segurança da Informação visam preservar a integridade, confidencialidade e disponibilidade das informações do Grupo BR Partners:

- Confidencialidade: garantia de que a informação é acessível somente a pessoas autorizadas;
- Integridade: salvaguarda da exatidão e completude da informação e dos métodos de processamento; e
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Descrição de uma conduta adequada e segura para o manuseio, controle e proteção das informações contra destruição, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

Este Manual da Política é aplicável a todas as informações sob gestão do Grupo BR Partners, que podem existir de muitas maneiras: escrita em papel, armazenada e transmitida pelo correio ou por meio de meios eletrônicos, exibida em filmes ou falada em conversas formais ou informais. Seja qual for a forma apresentada ou o meio do qual a informação seja apresentada ou compartilhada, deverá estar sempre protegida adequadamente, de acordo com controles definidos neste Manual.

As informações de propriedade ou controladas pelo Grupo BR Partners devem ser utilizadas apenas para uso próprio de propósitos definidos. Os usuários não podem, em qualquer tempo ou sob qualquer propósito, apropriar-se dessas informações para uso próprio.

De acordo com a Política de Segurança da Informação do Grupo BR Partners sempre que o usuário encontrar informações, aplicações ou procedimentos críticos sem o tratamento de segurança correto, deverá informar seu superior imediato para que sejam tomadas providências necessárias.

O não cumprimento das regras da Política de Segurança da Informação do Grupo BR Partners acarretará em punição conforme previsto nas políticas internas.

4.2. Internet Corporativa

O serviço de Internet é disponibilizado exclusivamente para uso nas atividades profissionais. O acesso às páginas da Internet, por meio dos recursos disponibilizados pelo Grupo BR Partners, caracteriza um instrumento de trabalho e, assim destina-se e limita-se à execução das atividades pertinentes à função.

O acesso à Internet, por meio da rede corporativa, deve ser efetuado somente por equipamentos autorizados pela área de Tecnologia. A conexão à internet deve ser encerrada sempre que o usuário se ausentar de sua estação de trabalho ou ao término do uso da sessão.

O acesso à Internet é controlado e monitorado via Sistema de Firewall com URL Filtering e *Web Control integrado*. O conteúdo é acessado através de categorias que são liberadas com a anuência da área de *Compliance*, além de análise do protocolo HTTPS para verificação de pacotes criptografados representam ou não uma ameaça, ou seja, se o dado é malicioso ou não, se deve ser exibido no navegador. Além disso, o filtro de conteúdo impede o acesso a páginas indevidas de conteúdo malicioso, vírus e ameaças à segurança da informação, pois recebe atualização *on-line* sobre categorização de sites e conteúdo.

O Grupo BR Partners reserva-se o direito de examinar e de monitorar o acesso a Internet disponibilizada, em conformidade com os termos da Lei e de utilizar do conteúdo das trilhas de auditoria, sendo proibido:

- Utilizar os recursos do Grupo BR Partners para fazer *downloads* (mp3, vídeos, programas diversos) de conteúdo que não seja para utilização no trabalho, distribuição de *software* de qualquer natureza e de dados não legalizados, bem como a distribuição destes;
- Divulgar informações confidenciais do Grupo BR Partners ou de seus clientes em grupos de discussão, fóruns, listas ou bate-papo e afins, 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;
- Acessar informações ilegais ou que possam ser consideradas ofensivas, intimidatórias, ameaçadoras ou similares, sendo que o usuário será responsabilizado pelos sites acessados e pelos arquivos copiados para a rede interna da Instituição;
- Acessar portais ou páginas com conteúdo de caráter obsceno, sexual, pornográfico, erótico, racista, constrangedor, difamatório, discriminatório ou preconceituoso (sexo, raça, etnia, religião, nacionalidade), ilegal, agressivo e abusivo ou de qualquer outra natureza, que atente contra a integridade moral e os bons costumes dos indivíduos ou de grupos da sociedade;
- Copiar programas *freeware*, *shareware* ou que não tenham sido adquiridos pelas formas legais e conformidade com as leis brasileiras e autorizado pela área de

Tecnologia. A utilização de *softwares* não legalizados é considerada pirataria e pode causar danos financeiros e de imagem para o Grupo BR Partners;
- Utilizar *softwares* de troca de arquivos nos formatos *peer-to-peer* (P2P) ou *torrent*;
- Utilizar serviços de *streaming*, tais como rádios *on-line* e afins, a não ser que o acesso seja inerente a trabalhos, pesquisas ou negócios do Grupo BR Partners;
- Utilizar *softwares* de comunicação instantânea não homologados pela Tecnologia e previamente autorizados por *Compliance*;
- Acessar e propagar qualquer tipo de conteúdo malicioso, como vírus, *worms*, cavalos de tróia ou programas de controle de outros computadores, bem como spam;
- Utilizar para jogos *on-line*, fóruns não profissionais, gincanas e concursos *on-line*;
- Utilizar a rede para fins comerciais, ilegais ou imorais;
- Utilizar para tentativa de ataque ou intrusão a outros computadores da rede interna ou externa;
- Utilizar para cópia, distribuição ou armazenamento não autorizado de material ou *software* protegido por leis de direito autoral, por qualquer meio;
- Utilizar *webmail* particular ou mesmo instalar a conta de e-mail particular para utilização no cliente do *desktop c*orporativo; e
- Disponibilizar a outro usuário sua conta de acesso, devendo seu *login* e sua senha ser tratados de forma particular, confidencial e exclusiva.

Caso a área de Tecnologia e Segurança da Informação julgue necessário poderá efetuar bloqueios de acesso a arquivos, domínios e serviços de Internet que comprometam o uso de banda, a segurança do Grupo BR Partners ou o bom andamento dos trabalhos. Com base em relatórios para análise de segurança dos sites acessados pelos Colaboradores poderá haver restrição a determinados conteúdos/sites sem aviso prévio.

O Grupo BR Partners disponibiliza uma rede w*ireless* sem restrições de acesso para uso de clientes e equipamentos pessoais, esta rede é fisicamente apartada da rede corporativa. Algumas áreas da empresa podem ter restrições quanto ao uso de equipamentos particulares, dependendo da área de atuação.

4.3. Correio Eletrônico

O Correio Eletrônico é uma ferramenta essencial ao dia a dia, permitindo agilidade na comunicação interna e externa. As mensagens e os documentos eletrônicos estão sujeitos às mesmas leis e normas aplicadas a documentos escritos. O uso não controlado ou inapropriado desta ferramenta pode trazer ameaças reais, tais como:

- Criminal;
- Autoridades Regulatórias;
- Contaminação por Vírus;

- Quebra da Confidencialidade; e
- Danos a Imagem.

Assim, como qualquer recurso provido pelo Grupo BR Partners, o uso dos serviços do correio eletrônico deve ser dedicado às atividades de interesse do Grupo regido por regras de conduta similares àquelas aplicáveis a outros recursos de informática. O uso adequado deve ser legal, ético, refletir honestidade e demonstrar moderação no consumo dos recursos compartilhados. O uso inapropriado dos serviços de correio eletrônico, em alguns casos, pode causar interrupção das atividades da instituição.

As mensagens enviadas por meio do e-mail corporativo não são consideradas como informação particular. Assim sendo, o Grupo reserva para si o direito de monitorar e inspecionar o uso do e-mail disponibilizado, em conformidade com os termos da Lei.

Todas as mensagens ficam armazenadas em um servidor que possui recursos limitados. Para que não ocorram problemas de indisponibilidade de caixas postais, o Colaborador deve periodicamente excluir as mensagens que não forem mais necessárias para liberar espaço na Caixa Postal e permitir que continue a receber mensagens.

Todas as mensagens deverão ser salvas em pastas dentro do próprio aplicativo disponibilizado Microsoft Outlook, não sendo permitido salvá-las no desktop local, pois não é efetuado backup dos dados salvos localmente no desktop corporativo.

Todos os dados trafegados no e-mail sejam mensagens, arquivos ou chat são monitorados por ferramenta CASB provendo rastreabilidade dos dados trafegados na plataforma de e-mails adotada o Microsoft Office 365.

Poderá ser dado a um usuário o direito de acessar a caixa postal de outro usuário mediante autorização da Pessoa por e-mail, desta forma a Tecnologia liberará este acesso. Este procedimento pode ser realizado pelo usuário proprietário da caixa postal ou pela área de Tecnologia por meio de autorização por escrito do proprietário da caixa postal ou seu superior.

Não há qualquer procedimento específico (desativação, exclusão, etc.) para casos de ausência temporária (férias, licença-prêmio, licença sem vencimento, etc.). Caso deseje, o usuário poderá configurar sua caixa postal para deixar de receber mensagens.

Só é permitida a criação de caixa postal para terceiros (fornecedores, prestadores de serviços, etc.), mediante autorização previa da gerência, diretoria e área de Tecnologia por meio do Formulário de Solicitação de Liberação de Acesso.

Os colaboradores demitidos ou afastados terão a caixa postal bloqueada imediatamente e no período de até 2 (dois) meses a mesma será desativada ou excluída completamente para casos de desligamento.

Não obstante é expressamente proibido aos colaboradores:

- Transmitir material que seja considerado ofensivo, discriminatório, calunioso, fraudatório, danoso, ilegal ou que possa violar os padrões de ética e cortesia profissional;
- Transmitir ou abrir material que contenha pornografia e conteúdo de assédio moral;
- Transmitir piadas e conteúdo humorístico;
- Transmitir arquivos executáveis como anexo e extensões que possibilitem a propagação de vírus: (.bat, .chm, .cmd, .dll, .dot, .elm, .exe, .hta, .inf, .js, .jse, .lnk, .pif, .scr, .vbs, .vxd). Esta lista está sujeita a alterações sem aviso prévio;
- Transmitir *spam* (mensagens não solicitadas enviadas para vários destinatários com conteúdo não relacionado às atividades do Grupo BR Partners, como, por exemplo: divulgação comercial, autopromoção, etc.);
- Participar de "pirâmides" e "correntes" (correspondência não relacionada aos negócios da empresa que seja replicada para muitos usuários); Retransmitir e-mails atachados com anexos não relacionados ao conteúdo corporativo, os quais podem interromper ou prejudicar o funcionamento dos servidores/equipamentos de outra pessoa ou causar problemas de performance no sistema. Lembrando que não é possível o tráfego de e-mails com tamanho maior que 35MB;
- Abrir arquivos atachados de origem duvidosa;
- Colocar seus e-mails em chats e listas de discussão não relacionadas ao trabalho;
- Colocar as suas opiniões pessoais como sendo aquelas do Grupo BR Partners;
- Divulgar informações consideradas confidenciais ou proprietárias do Grupo BR Partners ou de seus clientes, enviar a terceiros informações relativas às atividades do Grupo BR Partners e de suas missões e transações, exceto quando aprovadas formalmente pela diretoria, reenviar a terceiros comunicados recebidos quando expressamente não permitido; e
- Divulgar o endereço de e-mail de outros funcionários sem a anuência dos mesmos.

O Grupo BR Partners se reserva o direito de preservar seus equipamentos e recursos computacionais através da recusa do recebimento de mensagens cujos conteúdos não expressam o interesse do Grupo BR Partners, ou que possam colocar em risco o funcionamento dos sistemas.

As caixas postais do correio eletrônico, incluindo as informações contidas em seus arquivos, são propriedade do Grupo BR Partners, reservando-se ao mesmo, portanto, o direito de monitorar e gravar toda a atividade quando considerar necessário. O uso da caixa postal de correio eletrônico e dos demais recursos de informática indica o consentimento do usuário a essa monitoração e, quando necessário, à divulgação do Grupo BR Partners às autoridades competentes de quaisquer evidências que possam constituir crime, delito ou violação às atividades. O Grupo BR Partners poderá eventualmente realizar monitoração (auditoria) das caixas postais através da utilização de *softwares* específicos.

Todas as mensagens são passíveis de monitoração e gravação quanto aos endereços de destino e origem (IP de origem, E-mail do remetente, IP de destino, E-mail do destinatário) e poderão ser usados para estabelecer critérios de recusa.

Eventuais ações de leitura de e-mail pela administração do sistema podem ocorrer perante autorização do responsável pela caixa postal ou do gestor.

Para os casos de falha ou incompletude dos procedimentos previstos, bem como, no enfrentamento de situações inesperadas, a área de Tecnologia poderá, a seu critério, suspender a conta de correio ou todo o serviço comunicando o fato à Diretoria.

4.4. Acesso Físico e Lógico

Os colaboradores do Grupo BR Partners devem ter acesso físico e lógico liberado somente aos locais e recursos necessários ao desempenho de suas atividades e de conformidade aos interesses da empresa.

O acesso físico às dependências do Grupo BR Partners é controlado mediante cartão magnético e autorizado pela área de *Compliance*. Todos os ambientes operacionais possuem dispositivos de leitura de cartão, e visitantes que necessitem de acesso aos locais devem obrigatoriamente ser acompanhados por um colaborador autorizado.

O Datacenter está em espaço reservado, com todos os controles de acesso e ambientais necessários ao bom funcionamento do ambiente. Somente a equipe de Tecnologia possui autorização de acesso. Qualquer fornecedor ou terceiros que necessitem ter acesso ao Datacenter, devem ter autorização de acesso e serem acompanhados por colaborador da equipe de Tecnologia.

O acesso à rede interna somente será realizado por meio das estações de trabalho, sendo que esses equipamentos serão controlados para eliminar possíveis riscos de vulnerabilidades, vírus e garantindo o cumprimento da política de utilização de *softwares*.

O procedimento formal de registro, mudança de colaborador de departamento/área e cancelamento de usuário para obtenção, alteração de privilégio e remoção de acesso a todos os sistemas de informação, a rede corporativa, bases de dados e a serviços necessários para o bom desempenho de sua atividade é realizado por meio da solicitação do gestor da área comunicando às áreas de *Compliance,* Tecnologia e Recursos Humanos, conforme as informações descritas no Formulário de Solicitação de Acesso, assegurando a segregação de funções e a segurança da informação.

Para acesso aos equipamentos e sistemas aplicativos ligados à rede do Grupo BR Partners, cada usuário deverá identificar-se por meio de senha. A senha é de uso pessoal e intransferível.

Para que haja maior segurança nas estações de trabalho, o usuário deverá observar as seguintes determinações:

- Toda vez que for se ausentar da sua mesa de trabalho, o usuário deverá, preferencialmente, bloquear sua estação da seguinte forma:
- Pressionar, ao mesmo tempo, as teclas "CRTL+ALT+DEL"; e
- Clicar na opção "Bloquear computador" ou pressionar ao mesmo tempo a Tecla "WINDOWS + L".

Todo equipamento que permanecer sem utilização por 10 (dez) minutos seguidos será automaticamente bloqueado e a proteção de tela ativada, salvo em estações de usuários com privilégios específicos.

A data e hora das estações de trabalho não poderão ser alteradas pelos usuários, sendo estas sincronizadas com os servidores automaticamente.

Qualquer componente de *hardware* do equipamento de cada usuário só poderá ser instalado, trocado ou removido pela área de Tecnologia. Os usuários somente poderão utilizar os *softwares* instalados pela área de Tecnologia, não podendo instalar novos, alterar ou remover os existentes.

Os *desktops* deverão ser desligados pelos usuários após o seu expediente de trabalho, garantindo assim a conservação física e lógica, bem como a prevenção, no caso de ocorrência de algum problema elétrico ou na manutenção da rede.

A área de Tecnologia (administrador da rede LAN e/ou seus prepostos) deverá efetuar o controle de acesso, de acordo com os privilégios definidos, por meio do Sistema de Administração da Rede, bem como a manutenção do cadastro dos colaboradores através da informação da área de Recursos Humanos sobre as movimentações (desligamento e transferências) de colaboradores.

Os registros de acesso somente poderão ser acessados pelo administrador da rede e/ou seus prepostos.

A área de Tecnologia deverá instalar em todos os equipamentos, antes de sua utilização pelo usuário, *softwares* de detecção e proteção contra "vírus" (vacinas).

4.5. Senhas de Acesso

Toda senha é de caráter pessoal, secreta e intransferível. Cada usuário é inteiramente responsável pela guarda e utilização de sua senha.

O compartilhamento de senhas será considerado como falta grave e passível de sanções disciplinares. Neste caso, a área de Tecnologia efetuará o bloqueio do acesso e comunicará a Diretoria.

As senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a rede ou a um sistema de informação ou serviço.

Para nenhuma finalidade é permitida a utilização de programas maliciosos para descobrir ou quebrar senhas de arquivos e programas.

A senha deverá ser alterada a cada 45 (quarenta e cinco) dias corridos, sendo que a mesma não poderá ser repetida nas próximas 6 (seis) alterações. Não obstante, o colaborador poderá alterar a sua senha, a qualquer momento, não sendo necessário aguardar os 45 (quarenta e cinco) dias entre as trocas.

A formação da senha deverá ser efetuada pelo próprio Colaborador, sendo composta por:

- no mínimo, 8 (oito) caracteres de comprimento;
- nesses 8 (oito) caracteres alfanuméricos é obrigatório conter, no mínimo, 1 (um) número, 1 (uma) letra maiúscula, 1 (uma) letra minúscula ou 1 caractere especial. A senha deve conter caracteres de 3 (três) das 4 (quatro) categorias citadas; e
- Bloqueio da Senha após 3 (três) tentativas. O desbloqueio será efetuado somente pela Tecnologia no ramal 1033.

Para a formação da senha, o usuário deverá tomar alguns cuidados para que não seja facilmente identificada por terceiros, como por exemplo, não utilizar:

- Nomes de cônjuges;
- Nomes de filhos;
- Data de nascimento;
- Anagramas (palavra ou frase formada pela transposição das letras de outra);
- Palavra ou frase, exemplo, Belisa (Isabel), Avalor (Álvaro), Arima (Maria);
- Números de documentos pessoais; e
- Nunca usar uma senha igual ao nome do usuário.

Após a formação da senha, a mesma deverá ser memorizada pelo usuário. É expressamente proibida a impressão ou manutenção da senha anotada, assim como a divulgação da mesma a terceiros.

A área de Tecnologia não pode solicitar e não necessita de sua senha para realizar qualquer atendimento.

Além de senha de acesso toda conta atrelada ao Office 365 deverá estar habilitado o MFA (autenticação de múltiplo fator)

4.6. Utilização de *File Server* Corporativo

É obrigação do usuário segmentar e gravar os documentos sempre na pasta da área correspondente, não podendo armazenar documentos da empresa na pasta pessoal Z. Possuem *backup* somente os documentos salvos na rede, os documentos salvos no *desktop* local não entram na política de *backup*, portanto não tem cópia de segurança.

Deve-se obedecer a política de cota de disco implantada no drive Z ao limite de 2GB de espaço em disco.

4.7. Utilização de *Software*

O Grupo BR Partners concede a seus colaboradores, juntamente com os servidores, *desktops*, *notebooks* e demais recursos disponíveis do seu patrimônio, a concessão de utilização *de softwares*, devidamente licenciados para o desempenho de suas atividades.

Todo *software* utilizado pelo Grupo BR Partners tem seu direito de uso devidamente licenciado de terceiros. Salvo formalmente autorizado por um fornecedor oficial, o Grupo BR Partners não tem o direito de reproduzir *software* e manuais em seu poder, com exceção à montagem de cópias de segurança (*backup*) sob responsabilidade da área de Tecnologia.

Com relação ao uso em redes ou em máquinas multiusuários, os colaboradores do Grupo BR Partners somente deverão usar o *software* de acordo com a licença acordada. O número de cópias simultaneamente em uso não poderá ultrapassar o contratado com o fornecedor.

A contratação de serviços correlatos à Tecnologia, sob qualquer pretexto, tem que ser previamente submetidas à análise dos departamentos Jurídico e de Tecnologia. Somente é permitida a utilização de *softwares* homologados e licenciados através da área de Tecnologia. Caso ocorra alguma necessidade de utilização de algum *software* que não esteja homologado, deverá ser solicitada a área de Tecnologia, onde todos os procedimentos de homologação e legalização serão realizados.

Fontes, imagens gráficas, programas *free* como Adobe, Pkzip, Babylon, Imposto de Renda são considerados *softwares*, devem ser homologados e terem os direitos de uso autorizados pela área de *Compliance* e Tecnologia. A área de Tecnologia é responsável por:

- Avaliar a necessidade de aquisição de *softwares*, bem como a sua compatibilidade;
- Proceder à instalação dos softwares adquiridos pelo Grupo BR Partners;
- Efetuar a transferência de software entre áreas ou entre computadores da mesma área;
- Manter em local apropriado e em segurança os discos originais e seus *backups* (cópias de segurança), bem como os respectivos manuais e contratos de cessão de

uso; e

- Acompanhar, juntamente com o usuário, o prestador de serviço, quando de atualizações de software/hardware, apresentações de novos aplicativos etc.

O Grupo BR Partners reserva para si o direito de realizar inventários em seus ativos.

Considerando que a Lei nº 9.609/98, disciplinou a proteção da propriedade intelectual sobre programas de computador, todos os deverão observar rigorosamente o disposto nesta lei, sob pena de incidirem nas sanções previstas na aludida norma federal.

Os colaboradores do Grupo BR Partners que identificarem alguma irregularidade no uso de *software* ou na respectiva documentação deverão notificar a área de Tecnologia.

4.8. Utilização de *Notebooks* e Dispositivos Móveis

O Grupo BR Partners disponibiliza a cada colaborador um equipamento para uso individual. De acordo com as funções de cada área, este equipamento pode ser um *desktop* ou, adicionalmente, uma *workstation*. Estes equipamentos fazem parte do patrimônio do Grupo BR Partners e é expressamente proibido retirá-lo das dependências da empresa, com exceção daqueles destinados a esta finalidade.

Qualquer *notebook*/*desktop* pessoal ou de visitantes da empresa não poderá adentrar a rede corporativa do Grupo BR Partners. Toda mídia de origem externa como por exemplo pen drive, DVD e etc deve ser submetida à área de Tecnologia antes de ser conectado nos equipamentos para que seja feito um Scan contra ameaças como vírus e etc.

O uso do e-mail através *webmail* deve respeitar as mesmas normas de utilização do correio eletrônico corporativo, estando o usuário responsável pela manutenção da confidencialidade das informações assim como pelo bem-estar físico do aparelho fornecido. O chaveiro de Internet 3G deve ser utilizado somente em visita a clientes ou em situações de indisponibilidade total dos sistemas.

A política de segurança da informação deve ser aplicada também aos equipamentos particulares, sendo dever do usuário respeitá-la e sempre salvaguardar as informações pertencentes ao Grupo BR Partners.

4.9. *Política de Backup e Restore*

O sistema de *backup* é compatível com a complexidade dos negócios do Grupo BR Partners. O *backup* é realizado diariamente em ambiente de Produção, Homologação e Desenvolvimento utilizando robôs automatizados com drive de Fitas LTO 3 e 4 que são enviadas diariamente para guarda externa na empresa especializada INTERCON, em container apropriado para transporte de fitas e em carro com condições climáticas adequadas para este tipo de transporte.

O *backup* é realizado diariamente em ambiente de Produção, Homologação e Desenvolvimento utilizando robôs automatizados com *drive* de Fitas LTO 3 e 4 que são enviadas diariamente para guarda externa respeitando o tempo de retenção definidos, sendo adotada a modalidade de *backup full*.

São utilizadas 4 (quatro) periodicidades de *backup*: diário, semanal, mensal e anual.

As mídias ficam armazenadas em ambiente adequado conforme política de retenção que obedece aos critérios descritos abaixo:

- *Backup* Diário – Retenção de 14 dias
- *Backup* Semanal– Retenção de 30 dias
- *Backup* Mensal – Retenção de 5 anos
- *Backup* Anual– Retenção de 10 anos

As mídias com os *backups* diários e mensais dos bancos de dados são armazenadas com uma empresa, sob contrato com cláusulas de Acordo de Nível de Serviço (SLA), prevendo a sua disponibilização em até 2 (duas) horas para a cidade de São Paulo. O transporte das mídias é feito em veículos fechados, sem identificação e são acondicionadas em malas antichama e antichoque, lacradas e com controle de envio e recepção.

O prazo de *restore* de arquivos deverá ser o tempo definido no acordo de nível de serviço (SLA) assinado entre a Tecnologia e as áreas de Negócios.

Os procedimentos de *backup* e *restore* executados pela equipe de Tecnologia estão definidos no documento "Procedimento *Backup* - Normas e Procedimentos.docx" armazenado na pasta da área.

4.10. Política de Gestão de Mudanças (GMUD)

O processo de Gestão de Mudanças definido conforme documento "Gerenciamento de Mudanças" baseado em ITIL. Toda mudança a ser realizada é registrada no sistema *SysAid* e necessita ser planejada, aprovada pela área de negócios, e executada na data e horário programado. Assim, temos 2 (dois) tipos de mudanças:

- Normal (correções e implantações): executada de quinta e sexta-feira após o fechamento do mercado; e
- Emergencial (correções e implantações urgentes): em dia e horário acordados entre as equipes de Infraestrutura e Sistemas.

4.11. Política de Gestão de Incidentes, Problemas e Demandas

Documentar os procedimentos necessários para abertura, acompanhamento e fechamento dos incidentes, problemas e solicitações (demandas) via sistema *SysAid*:

- **Incidente:** Toda solicitação referente a acessos, correções, instalações seja em *software*, sistema ou *hardware*;
- **Problema**: Incidentes recorrentes, que são resolvidos de forma paliativos, são transformados em problemas para uma melhor análise para a correção definitiva; e
- **Solicitações (Demandas)**: Melhorias levantadas por usuários ou por fornecedores que são registradas para caso viáveis serem disponibilizadas.

4.12. Auditoria

Serão realizadas auditorias periódicas para verificação do grau de cumprimento desse Manual da Política. São consideradas razões empresariais legítimas, porém não limitadas:

- Identificar e diagnosticar problemas de *hardware* e *software*;
- Prevenir o uso incorreto do sistema;
- Investigar conduta imprópria ou ilegal, atividade antiética ou inadequada;
- Assegurar conformidade com os direitos de propriedade, licença e obrigações contratuais; e
- Proteger os interesses empresariais da organização.

5. REVISÃO

Este Manual da Política deverá ser revisado, no mínimo, anualmente.

6. DOCUMENTOS RELACIONADOS

Política de Segurança da Informação

Manual de Segurança Cibernética

7. LEGISLAÇÃO E REGULAÇÃO

Lei nº 9.609/98

Resolução nº 4.263/13 do Conselho Monetário Nacional (CMN)

Instrução nº 539/13 da Comissão de Valores Mobiliários (CVM)

Instrução nº 554/14 da Comissão de Valores Mobiliários (CVM)