MANUAL DE SEGURANÇA DA INFORMAÇÃO

BR·OFFICES

ANEXO II – MANUAL DE SEGURANÇA DA INFORMAÇÃO

- **Introdução**

Este Manual de Segurança das Informações foi desenvolvido com o intuito de estabelecer as diretrizes e melhores práticas necessárias para a proteção de nossas informações, bem como informações de terceiros armazenadas em nossa estrutura, principalmente as de clientes.
Nele estão contemplados um conjunto de princípios, práticas e cuidados mínimos necessários que norteia a gestão de segurança de nossas informações corporativas.
Este documento é aplicável a todos os funcionários, sócios, fornecedores, prestadores de serviços e parceiros comerciais do BR.Offices ("colaboradores") e será regularmente atualizado e divulgado pela área de Compliance, responsável também pelo monitoramento e estabelecimento de procedimentos e mecanismos de controles internos que visem à observância das disposições aqui contidas.
Em linha com as expectativas da diretoria executiva do BR.Offices, é responsabilidade de todos a implementação e o cumprimento das regulamentações aplicáveis sobre o tema e de todo o conteúdo deste Manual. Como colaborador do BR.Offices, para assegurar a eficácia dos procedimentos e controles transcritos ao longo deste documento, você deve tomar conhecimento sobre suas funções e responsabilidades específicas sobre o assunto, bem como zelar pelo cumprimento das mesmas.

- **Objetivo e Abrangência**

Este Manual foi desenvolvido com o objetivo de definir regras, responsabilidades e estratégias essenciais relacionadas aos procedimentos e mecanismos de controles internos relacionados à segurança da informação, visando minimizar os impactos associados à ação de ameaças e riscos em todo o "ciclo de vida de cada informação". A abrangência das regras e controles aqui dispostos refere-se ao ciclo de vida físico e lógico da informação, conforme ilustrado e detalhado abaixo:

Fase / Meio	Meio Físico	Meio Lógico
Criar	Documentos gerados e disponibilizados pelo BR.Offices.	Bases de dados e informações geradas e disponibilizadas pelo BR.Offices.
Transmitir	Documentos (inclusive mídias móveis) que circulam internamente ou aqueles recebidos e enviados (externamente).	Transmissão ou recebimento de arquivos e informações eletronicamente (ou por telefonia)
Manusear	Uso e acesso a informações e dados físicos (inclusive mídias móveis).	Uso e acesso a informações e dados lógicos (inclusive mídias móveis).
Armazenar	Formas de acesso e organização do armazenamento de documentos e mídias em locais físicos internos ou externos.	Arquivos de dados de documentos e informações eletrônicas.

Descartar	Fragmentação de documentos físicos e mídias.	Exclusão de dados e informações lógicas.

- **Classificação das Informações**
    - As informações são divididas em 02 (dois) grandes grupos:

- GRUPO 1: Informações de clientes;
- GRUPO 2: Informações corporativas (incluindo informações de produtos e serviços).

O acesso a essas informações se dará em relação aos seguintes níveis: **CONFIDENCIAL, RESTRITO, INTERNO e PÚBLICO.**

Confidencial – As informações de acesso CONFIDENCIAL são aquelas que, uma vez divulgadas ou acessadas por pessoas não autorizadas podem expor o BR.Offices de maneira gravíssima, devendo ser tratadas com um rigor mais assentuado, divulgando-as somente às autoridades públicas competentes e desde que preceda de ordem judicial nesse sentido. São exemplos de informações com nível de acesso confidencial: Toda e qualquer informação estratégica da empresa; toda e qualquer informação financeira da empresa; informações sobre a tecnologia aplicada nos processos do BR.Offices; correspondências recebidas enviadas a clientes.

Em relação a esse nível de acesso devem ser observadas as seguintes precauções:

- É vedada a divulgação fora da empresa ou mesmo internamente para pessoas que não necessitem de seu conhecimento para o exercício de suas funções (Need to Know Policy);
- O acesso é exclusivo ao reduzido número de colaboradores autorizados pelo Diretoria Executiva;
- Deve ser armazenada em local de acesso restrito e seguro;
- Quaisquer informações de clientes devem ser classificadas e tratadas como estritamente confidenciais assim como os relatórios de fiscalização, auditoria, rating, e de órgãos reguladores ou fiscalizadores.
- O acesso a informações desse nível será concedido pela Diretoria Executiva ou por pessoa por ela devidamente designada, devendo ficar apenas no nível Diretoria Executiva e Gerentes e *Compliance*, sendo vedada sua divulgação a todos os demais setores/departamentos.

Restrito – As informações de nível RESTRITO são aquelas que, uma vez acessadas por pessoas não autorizada podem acarretar danos, trazendo prejuízos graves ou moderados para o BR.Offices. São exemplos de informações de nível RESTRITO: cadastro e documentos de clientes relacionados ao cadastro; informações financeiras sobre os clientes; contratos firmados com terceiros.

Em relação a esse nível de acesso devem ser observadas as seguintes precauções:

- É vedada a divulgação fora da empresa ou mesmo internamente para pessoas que não necessitem de seu conhecimento para o exercício de suas funções (Need to Know Policy);
- As informações desse nível de acesso devem ser igualmente preservadas, em seu estado original, durante todo o período de necessidade de armazenamento.
- O acesso a informações desse nível será concedido pela Diretoria Executiva ou por pessoa por ela devidamente designada.

Interna – informação com acesso autorizado somente aos colaboradores que a necessita para o

exercício pleno de suas funções. Os danos ou prejuízos causados pela divulgação não autorizada são de impacto brando ou moderado para o BR.Offices. Deve, ainda, ser passível de controles básicos a fim de evitar que sua integridade seja abalada.

Pública – esta é de conhecimento irrestrito e pode ser divulgada fora da empresa, desde que sejam respeitadas as regras dispostas neste Manual e demais políticas e diretrizes internas.

Obs: Toda e qualquer informação, salvo as informações confidenciais, poderão ser utilizadas pela equipe de vendas desde que imprescindíveis e necessárias para a captação de novos clientes e a manutenção dos já existentes. As estratégias de marketing e divulgação serão sempre tratadas previamente com a Gerência de Relacionamentos e com a anuência Departamento de Compliance.

Caso o colaborador se depare com uma situação em que lhe seja solicitado acesso a informações (do tipo Confidencial, restrito e interna) relacionadas ao GRUPO 01 ou 02, fica autorizado a imediata consulta à Gerência de Relacionamento, ou ao Departamento de Compliance ou, ainda, à Diretoria Executiva, sob pena de sofrer as penalidades cabíveis.

- **Relevância e Integridade**

As informações serão tratadas, ainda, em relação à sua relevância e integridade. Os gestores responsabilizarão para que as informações já existentes chegue de maneira correta a cada um dos colaboradores que será responsável pelo seu manuseio. Por sua vez, tratando-se de informações novas ou inéditas para o colaborador/receptador este deverá agir de acordo com o nível de acesso concedido, conforme disposto no item 3.1.

Dessa forma, para o GRUPO 01 deverá agir da seguinte maneira:

Informação/solicitações recebidas	Ação
Documento novo de cliente	Lançar registro no sistema. Enviar email ao cliente, arquivar em pasta física própria e armazená-la em local apropriado.
Solicitação de acesso a informações do cliente por autoridade pública	Pedir para se identificar. Tirar cópia do documento funcional, se possível. Solicitar o inteiro teor do mandado. Ler o inteiro teor e conceder acesso somente àquelas informações que constam no mandado. Registrar a visita da autoridade no sistema, indicando o cliente ou terceiro fiscalizado. Em caso de dúvida, solicitar imediato auxílio do superior ou, na ausência deste, da diretoria.
Solicitação de acesso à informações pelo próprio cliente	Solicitar documento de identificação. Confirmar dados no sistema. Conceder acesso somente ao que for solicitado. Caso a pessoa solicitante não conste no sistema, comunicar imediatamente ao responsável da que consta no sistema e negar acesso ao solicitante até que seja apresentada a autorização, a qual deverá ser escrita (por email, whasapp, de próprio punho). Conferir se a autorização está sendo concedida por pessoa devidamente autorizada.

Informações obtidas através do canal de denúnica (Compliance Officer)	Nessa situação o Compliance Officer deverá receber a informação e proceder com a análise de sua pertinência ou não, iniciando o Processo de Apuração Institucional-PAI quando necessário. Uma vez iniciado o processo este deverá ser conduzido até que se obtenha uma conclusão firma acerca da denúncia lançada. A conclusão obtida poderá resultar, para o colaborador, na aplicação de sansões trabalhistas e, para o colaborador e demais envolvidos, o encaminhamento da apuração para as autoridades competentes. Além disso, o próprio BR.Offices poderá ajuizar demanda em face dos envolvidos, em razão de situações que lhe atribuam legitimidade.

Para conceder acesso às informações novas/inéditas relacionadas ao GRUPO 02, o colabodorador deverá proceder cda seguinte forma:

Informação/solicitações recebidas	**Ação**
Informações obtidas após reuniões; documentos relacionados ao programa de integralidade, código de ética, e qualquer outro relacionado à empresa, incluindo as atualizações	Tomar pleno conhecimento do que lhe for apresentado, ler os documentos na integra e, em relação àquilo que for necessário, assinar. Guardar as informações consigo e somente divulgá-las quando autorizado. Quando tiver dúvidas sobre a divulgação dessas informações, deve solicitar a ajuda de seu superior e, na ausência deste, da Diretoria Executiva.
Solicitação de acesso a informações do cliente por autoridade pública	Pedir para se identificar. Tirar cópia do documento funcional, se possível. Solicitar o inteiro teor do mandado. Ler o inteiro teor e conceder acesso somente àquelas informações que constam no mandado. Em caso de dúvida, solicitar imediato auxílio do superior ou, na ausência deste, da diretoria.
Solicitação de acesso à informações por pretensos clientes (caso de venda)	Fornecer informações estritamente necessárias para o fechamento do negócio, conforme tratado em reunião própria em que se imporá os limites de acesso às informações estratégicas. Caso o cliente insista em obter determinada informação (know-how do negócio, p. ex.) avaliar sobre a pertinencia e, sempre que necessário, solicitar auxílio da Diretoria Executiva.

Solicitação de acesso à informações pelos clientes	Ao receber a solicitação o colaborador deve avaliar a sua pertinência em relação aos serviços prestados ao cliente. Caso tenha pertinência, poderá responder desde que não exceda os níveis CONFIDENCIAL e RESTRITO. Em caso de dúvida, deverá solicitar auxílio do superior ou da Diretoria Executiva.

Os procedimentos aqui eleitos visam manter a integridade das informações gerenciadas pelo BR.Offices e que estão sob sua responsabilidade, buscando minimizar prejuízos internos ou em relação a terceiros

- **Retenção**

Prazo que a informação deverá ficar armazenada, bem como quando e como poderá ser descartada ou destruída.
O BR.Offices adota como período mínimo de guarda o prazo definido pelas leis e normas aplicáveis às nossas atividades e, em alguns casos, define períodos de retenção mais restritivos que os próprios órgãos reguladores, conforme classificação prévia da informação.
As informações relacionadas ao GRUPO 01, especificamente no que se refere à documentação do cliente (correspondências, documentos diversos, dentre outros obtidos de terceiros), permanecerão armazenadas pelo prazo máximo de 02 (dois) anos após o encerramento do contrato. Após esse prazo os documentos serão eliminados.
Ainda no que se refere ao GRUPO 01, os documentos relacionados ao cadastro dos clientes (cópia de documentos pessoais, atos constitutivos, dentre outros) serão devidamente digitalizados e comporão a base de dados do BR.Offices, sendo o descarte realizado a critério único e exclusivo da Diretoria Executiva.

- **Tratamento e proteção dos ativos de informação**

A seguir, estão dispostas regras e diretrizes não exaustivas quanto à proteção e tratamento dos ativos de informação do BR.Offices e quaisquer dúvidas ou esclarecimentos devem ser imediatamente direcionados ao departamento de Gerência Administrativa.

- **Guarda de Informações**

  - Documentos classificados como confidenciais ou restritos, principalmente de clientes, devem ficar armazenados em locais (físicos ou lógicos) de acesso restrito, seguros e organizados quando não estiverem sendo utilizados;
  - Os locais destinados ao armazenamento de informações de clientes e demais informações corporativas restritas ou confidenciais devem ser monitorados através de câmeras de segurança, registro/análise de “logs” e controle de acesso rigoroso;
  - O período de armazenamento de informações, antes do descarte, deve respeitar os períodos legais aplicáveis ou de políticas e diretrizes internas mais restritivas;
  - Quaisquer informações lógicas devem ser armazenadas tão-somente na rede corporativa (REMOTO/Storage), ou seja, é vedada a gravação de arquivos no disco rígido local (Diretório “C:”) e, ainda, em qualquer tipo de mídia sem análise e autorização da área de Compliance;

- O e-mail não deve ser utilizado primariamente para guarda de informações;
- Os locais de arquivamento externo, seja de mídias ou documentos físicos, devem ter contrato formalizado, com acordos de SLA (Acordo de Nível de Serviço) definidos e serem objeto de processo de *due diligence* com visitas periódicas, conforme o caso;
- Documentos de qualquer classificação "esquecidos" nas impressoras ou em locais não apropriados por colaboradores serão identificados e os colaboradores passíveis das penalidades internas cabíveis;
- Documentos de qualquer classificação "esquecidos" nas impressoras compartilhadas ou em locais acessíveis aos clientes serão identificados e, caso o autor não seja identificado, serão incinerados;

O envio e recebimento de informações e documentos em meio físico de/para locais externos devem ser necessariamente protocolados e controlados quanto à entrada e saída do BR.Offices. O motoboy ou outro profissional de entrega deve assinar o "Recebido", bem como informar o respectivo CPF.

- **Acesso Físico e Lógico**

A credencial de acesso a qualquer meio lógico ou físico trata-se de um importante mecanismo de controle e segurança de nossos ativos de informação. A Gerência de Recursos Humanos, Manutenção e *Compliance* realizará a revisão dos perfis e dos acessos físicos e lógicos no mínimo anualmente ou sempre que necessário, de acordo com o procedimento interno definido para tal e respeitando-se a segregação de funções. As não conformidades eventualmente detectadas durante esses processos poderão ser discutidas pelo Gerência Administrativa.

Acesso Lógico

Os perfis de acesso devem respeitar a segregação de funções estabelecida pelas normas vigentes e regras internas;

- O gestor deve solicitar, no momento da contratação do novo colaborador ou da movimentação de área do colaborador antigo, os acessos necessários aos diversos sistemas do BR.Offices.
- Os colaboradores desligados deverão ter seus acessos revogados no momento imediato do desligamento;
- Todo profissional que tenha acesso aos sistemas de informação do BR.Offices é responsável por tomar todas as medidas necessárias a fim de impedir o acesso não autorizado;
- Adicionalmente à regra lógica de bloqueio automático das estações de trabalho, todos devem travar o acesso aos seus computadores (CTRL+ALT+DEL) quando se ausentarem do local físico de trabalho, independentemente do período de ausência.

Acesso Físico

- O crachá de acesso ao prédio e dependências internas é pessoal e intransferível;
- As demais formas de acesso físico (Ex. biometria) somente deverão ser concedidas para os colaboradores que necessitarem para o exercício das funções e conforme orientação da área de *Compliance*;
- Todos os acessos biometricos possuem níveis de acesso diferenciados conforme cargo e/ou função a fim de evitar conflito de interesses e acesso não autorizado de informações. O nível de acesso é denifido pelo Diretoria Executiva e concedida pessoalmente a cada um dos colaboradores;

Grupo	Subgrupo	Descrição	Acesso	Horário

1	1	Cliente eventual	Nenhum acesso	
1	2	Clente Planos executivos	Acesso a Lounges e ambientes de reuniões.	Comercial
1	3	Clientes de CWK	Acesso a porta principal, lounges, copas, ambientes de reuniões e Coworking	24x7
1	4	Clientes de Offices	Acesso a porta principal, lounges, copas, ambientes de reuniões e sala contratada	24x7
2	1	Diretoria	Acesso ilimitado	24x7
2	2	Gerencia	Acesso ilimitado	24x7
2	3	Secretáriado	Acesso a porta principal, lounges, copas, ambientes de reuniões, ambientes restritos BROffices (correspondência, contrato, depósito, descanso, área administrativa)	Horário comercial
2	4	Copa/limpeza	Acesso a porta principal, lounges, copas, ambientes de reuniões, salas dos offices. Acesso aos ambientes restritos BR.OFFICES, apenas com supervisão)	Horário comercial

2	5	Manutenção	Acesso a porta principal, lounges, copas, ambientes de reuniões, salas dos offices e acesso aos ambientes restritos BR.OFFICES, com limitação do ambiente de correspondências e contratos)	24x7
2	6	vendas	Acesso a porta principal, lounges, copas, ambientes de reuniões	Horário comercial

- O registro supracitado deve conter, no mínimo, nome, CPF, contrato, empresa e grupo de acesso autorizado;
- **Grupos de acesso:**

Grupo	Subgrupo	Descrição
1	1	Cliente eventual
1	2	Clente Planos executivos
1	3	Clientes de CWK
1	4	Clientes de Offices
2	1	Diretoria
2	2	Gerência
2	3	Secretáriado
2	4	Copa/limpeza
2	5	Manutenção
2	6	Vendas

-
- Qualquer terceiro ou visitante deve aguardar, obrigatoriamente, em sala de espera ou na sala de reunião previamente agendada pelo cliente BR.Offices e, na hipótese de acessar uma área restrita deve estar devidamente acompanhado pelo cliente ou por um colaborador BR.Offices;
- O crachá do visitante fornecido pelo condomínio do edifício, deve ser apenas para identificação e sem qualquer tipo de acesso permitido, salvo nos casos autorizados pela Diretoria e conforme orientação de Compliance;
- Arquivo com cadastro de clientes e correspondências, Data Center, área de Research, Financeiro dentre outras são de acesso restrito às pessoas destas áreas e demais profissionais autorizados pela Diretoria.

Acesso e Protocolo de Correspondências

As **correspondências e documentos recebidos** seguem o seguinte esquema de recebimento:

- Verificação do lacre, em decorrência no nível de classificação da informação.
- Identificação do destinatário e remetente.
- Protocolo em sistema – Informação ao cliente do recebimento do documento (hora, data e loca) automática no ato do protocolo.
- Armazenamento da correspondência em ordem decrescente conforme protocolo, em local restrito.

O protocolo:

Gerado em sequencia numérica segue o seguinte padrão:

- Sigla da unidade – 2 letras
- Ano corrente – 3 caracteres
- Sequencial numérico – 5 caratceres
- Identificação do lote – 1 caractere
- Código de barras

Entrega da correspondência ao destinatário/cliente: A pessoa autorizada a retirar a correspondência – conforme consta no sistema e é informado através de email ou outro tipo de autorização escrita - após se identificar assina de próprio punho o registro da entrega das correspondências listadas.

Política de Senhas

Conforme anteriormente mencionado, cumpre-nos ressaltar que a senha de acesso a qualquer meio lógico ou físico trata-se de um dos mais básicos e importantes mecanismos de segurança de nossas informações.

A fim de assegurar as melhores práticas relacionadas a este tema, seguem abaixo algumas das diretrizes que devem ser observadas por todos:

- A senha deve ser memorizada e é de uso pessoal e intransferível;
- O eventual uso ou acesso indevido é de total responsabilidade do detentor e titular da senha que deve tomar todas as precauções necessários para salvaguardá-la;
- A senha de acesso aos sistemas internos deverá seguir os critérios definidos pela gerência administrativa.;
- O compartilhamento de senhas somente será permitido em casos de indisponibilidade para uso individual e se aprovado prévia e formalmente pela gerência administrativa;
- Toda e qualquer senha, de acesso físico ou lógico, deverá ser imediatamente bloqueada em casos de desligamento e/ou demissão;
- Especificamente com relação à senha de acesso à rede corporativa, a política é a seguinte:
- Deve ter, no mínimo, 6 (seis) caracteres e atender, no mínimo, a 3 dos 4 grupos de caracteres abaixo citados: a) Letras maiúsculas (de A a Z); b) Letras minúsculas (de a a z); c) Algarismos (de 0 a 9); e d) Caracteres não-alfabéticos (Ex. !, #, @, #, %).
- Deverá ser alterada, compulsoriamente, a cada 12 (doze) meses;
- Não pode ser igual ou similar às 6 (seis) últimas utilizadas;
- Não pode conter seu nome completo ou o de sua conta;
- Em hipótese alguma será concedida senha de acesso a outro funcionário que não seja o próprio usuário;
-
- Especificamente com relação à senha de acesso as salas corporativas, a política é a seguinte:
- Deve ter 4 (quatro) caracteres numéricos.
- Não pode ser utilizados números sequências ou mesmo repetidos.
    - Ex. 1234, 2222,1111, 1122, etc.
- Especificamente com relação à senha de acesso aos aplicativos disponibilizados através de aplicações web/Mobile, para clientes BR.OFFICES:
- Deve ter, no mínimo, 6 (seis) caracteres e atender, no mínimo, a 3 dos 4 grupos de caracteres abaixo citados: a) Letras maiúsculas (de A a Z); b) Letras minúsculas (de a a z); c) Algarismos (de 0 a 9); e d) Caracteres não-alfabéticos (Ex. !, #, @, #, %).
    -

Mídias e Recursos Portáteis

- Mídias e recursos portáteis ou móveis devem ser controlados e registrados;
- Os funcionários usuários de recursos portáteis (incluindo telefones celulares) devem comprovar, através de um termo de responsabilidade, que tomarão todos os cuidados no transporte e utilização destes equipamentos conforme orientação da gerência administrativa;
- ;
- Ao cliente será informada a impossibilidade de instalação de softwares diferentes dos já instalados nas máquinas de uso compartilhado. Porém, mediante requerimento, poderá solicitar a liberação e instalação pela gerência administrativa, quando necessário à realização de suas atividades.
- Na hipótese de eventual extravio/furto/roubo do equipamento celular de uso corporativo, o ato deverá ser imediatamente comunicado à gerência adminsitrativa para que seja realizado o bloqueio do equipamento/acesso.

- **E-mail e Telefonia**

Conforme disposto em nosso Código de Ética e Conduta, o BR.Offices fornece sistemas de comunicação eletrônica e por voz, tais como e-mail, telefones fixos e celulares, para fins profissionais.
Em relação ao uso do e-mail e comunicação por voz, todos devem observar as seguintes regras abaixo transcritas:

- O uso para fim pessoal deve ser de caráter resumido e objetivo. Todavia, é proibido o uso para ganho pessoal, malas diretas, "correntes", ameaças, assédio, entretenimento, dentre outros considerados impróprios, ilegais ou desnecessários para as atividades diárias;
- O correio eletrônico não pode ser utilizado, sem aprovação da gerência adminsitrativa, para envio ou recepção de mensagens que contenham arquivos executáveis, macros ou sequencias de comandos, explícitas ou implícitas, ou ainda outros mecanismos que possam conter vírus e, portanto, possam causar dano físico ou lógico aos equipamentos do BR.Offices ou de seus destinatários;
- E-mails de remetentes ou assuntos desconhecidos não devem ser abertos em nenhuma hipótese, sendo imediatamente reportados às áreas de Compliance.
- O uso do webmail corporativo e acesso remoto à rede e arquivos somente são concedidos a alguns colaboradores e mediante aprovação prévia da gerência administrativa;
- Todos os arquivos que são enviados e recebidos devem passar por um "filtro de e-mail" controlado e monitorado pelo Departamento de *Compliance*;
- Todos os E-mails encaminhados pelo serviço de webmail disponibilizado pelo BR.Offices deve conter a assinatura digital padrão da instituição.
- Definir assinatura digital (SUZANE)
- Os serviços de e-mail providos pelo BR.Offices *possuem* algumas restrições que visam manter a qualidade e a disponibilidade do serviço e da infra-estrutura que compõe a área de TI. São elas:
- (i) Tamanho máximo de arquivo em anexo: 25MB (25 Megabytes), salvo raras exceções, que possuem configuração compatível com tamanho máximo de10MB;

- (ii) Sistemas de Anti-Virus e Anti-Spam são atualizados diariamente e apagam os e-mails que contenham vírus e colocam em quarentena os que forem classificados como spam;
- (iii) Limite máximo de 25 destinatários;
- (iv) Capacidade máxima de 30G de armazenamento de Caixa-Postal, salvo raras exceções, que possuem configuração compatível com capacidade máxima de 10G.

- **Uso da Internet**

O uso da Internet pelos empregados do BR.Offices é permitido e encorajado desde que seu uso seja aderente aos objetivos e atividades fins do negócio da Empresa. Entretanto, o BR.Offices tem uma política para o uso da Internet desde que os funcionários/colaboradores assegurem que cada um deles:

- Siga a legislação corrente (sobre pirataria, pedofilia, ações discriminatórias);
- Uso razoável da Internet, sempre prezando pelo bom senso quanto aos sites acessados e tempo de utilização;
- Não crie riscos desnecessários para o negócio do BR.Offices.
- É estritamente proibido e inaceitável visitar sites da Internet que contenha material obsceno e/ou pornográfico;
- usar o computador para executar quaisquer tipos ou formas de fraudes, ou software/música pirata;
- usar a Internet para enviar material ofensivo ou de assédio para outros usuários;
- baixar (download) de software comercial ou qualquer outro material cujo direito pertença a terceiros (copyright), sem ter um contrato de licenciamento ou outros tipos de licenciamento;
- atacar e/ou pesquisar em áreas não autorizadas (Hacking);
- criar ou transmitir material difamatório;
- executar atividades que desperdice os esforços do pessoal técnico ou dos recursos da rede;
- introduzir de qualquer forma um vírus de computador dentro da rede corporativa.

Monitoramento

O BR.Offices reafirma que o uso da Internet é uma ferramenta valiosa para seus negócios. Entretanto, o mau uso dessa facilidade pode ter impacto negativo sobre a produtividade dos funcionários e a própria reputação do negócio. Em adição, todos os recursos tecnológicos do BR.Offices existem para o propósito de seu negócio que envolve o compartilhamento com seus clientes.

Assim, todo e qualquer acesso é monitorado pela gerência administrativa e pelo Departamento de Compliance, não havendo qualquer privacidade em relação ao tráfego de dados utilizados nas estações de trabalho dos colaboradores, tudo de modo a facilitar a transparência e o controle das atividades.

- **Utilização de Software**

Toda instalação de software deve ser feita pelo departamento de suporte e todos os softwares e aplicativos devem ser homologados e licenciados. Softwares instalados pela Internet, CD-

ROM ou qualquer outro meio de mídia magnética, diretamente pelo usuário ou por terceiros em qualquer equipamento ligado à rede do BR.Offices, sem conhecimento do departamento de suporte, e não considerado de interesse do BR.Offices, ou que infrinjam as regras desta política, podem ser desinstalados pela equipe de suporte sem aviso prévio.

A utilização de softwares fora dos padrões (como navegadores), bem como softwares livres ou temporários e sendo a sua utilização necessária, deverão ser tratados como exceções e deverão ser autorizados pelo responsável do departamento de suporte, desde que não prejudique o funcionamento de sistemas ou inflijam alguma regra, avisos ou boletins de segurança.

Os mesmos deverão ser revisados trimestralmente. A utilização de softwares não licenciados é considerada uma Não-Conformidade Gravíssima e acarretará punições ao funcionário ou colaborador, em qualquer nível, do BR.Offices. Todo parque tecnológico é mantido nas versões mais atuais desde que compatíveis com diversos Recursos Tecnológicos existentes e livres de falhas e erros que prejudiquem o uso em condições aceitáveis.

- **Descarte de Informações**

Toda informação que não necessite de sua manutenção em arquivos deve ser descartada, depois de decorrido o prazo legal, observando as diretrizes deste Manual, somente através de máquinas fragmentadoras (neste caso, somente para as classificadas como confidenciais ou restritas) e/ou conforme orientação da área de Compliance.

Adicionalmente à vedação de uso do e-mail para armazenamento primário de mensagens e arquivos, ressaltamos que todos os colaboradores devem adotar a prática de apagar mensagens (principalmente as que contenham arquivos anexados) antigas ou desnecessárias.

- **Comunicação Verbal**

Os colaboradores devem adotar cuidados especiais para evitar o comprometimento da segurança das informações através da comunicação verbal.

- É vedado tratar sobre assuntos confidenciais, restritos ou internos em locais onde estejam presentes pessoas não autorizadas. Adicionalmente, recomenda-se fortemente não gravar mensagens com conteúdo confidencial ou restrito em secretárias eletrônicas, caixas postais e afins;
- Informações classificadas como confidenciais não devem ser comunicadas por telefone.

- **Incidentes de Segurança**

Em caso de ocorrência de um vazamento de informações ou incidente de segurança, o colaborador deve registrar e comunicar o fato imediatamente à área de Compliance.

- **Resumo das principais vedações não excluídas todas as disposições contidas neste Manual**

- É proibido aos usuários da rede: Acessar, copiar ou armazenar programas de computador ou qualquer outro material (músicas, fotos e vídeos) que violem a lei de direitos autorais, bem como aqueles de conteúdo ilegal, pornográfico, discriminatório, homofóbico, racista, de apologia a crimes, dentre outros;
- Passar-se por outra pessoa ou esconder, por qualquer meio, a própria identidade quando utilizar os recursos computacionais ou quaisquer outros de propriedade do BR.Offices,

colocados à disposição do colaborador em razão do exercício de sua função;
- Usar ou divulgar informações confidenciais obtidas para benefícios pessoais (oportunidades de emprego, investimentos, dentre outros) mesmo após o término de seu vínculo com o BR.Offices;
- Alterar os sistemas padrões, sem autorização;
- Divulgar quaisquer informações confidenciais para concorrentes e/ou qualquer pessoa não ligada às atividades da Empresa;
- Efetuar qualquer tipo de acesso ou alteração não autorizada a dados dos recursos computacionais pertencentes à Empresa;
- Violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
- Acessar e-mail pessoal e serviços de mensagens instantâneas não autorizadas formalmente pelo Comitê de Segurança da Informação;
- Utilizar o telefone do BR.Offices para assuntos pessoais durante período de tempo não razoável;
- Criar blogs ou comunidades na Internet, ou qualquer ambiente virtual semelhante, fazendo uso, sem autorização expressa, da logomarca ou do nome do BR.Offices;
- Fazer uso do telefone celular e outros meios de comunicação e gravação particulares dentro das dependências do BR.Offices nos locais não autorizados;
- Uso ou instalação de softwares não licenciados e sem autorização da área de Tecnologia da Informação.

- **Treinamento**

Todos os colaboradores do BR.Offices deverão, além de aderir a este Manual, receber, periodicamente, treinamentos e materiais educativos que visem, principalmente, a conscientização e reciclagem de conhecimento de todos sobre o tema.
Novos colaboradores serão submetidos obrigatoriamente a um treinamento inicial acerca de suas funções e responsabilidades quanto ao assunto.
Essa mesma área efetuará o registro e o controle formal de presença, indicando a frequência e o tipo de treinamento ministrado, de modo a possibilitar o planejamento e a manutenção dos níveis mínimos de segurança.
Todos os treinamentos são preferencialmente ministrados por profissionais internos capacitados e diretamente ligados aos controles de segurança de informação do BR.Offices.

- **Considerações finais**

Todos os colaboradores devem atestar a leitura e perfeita compreensão deste documento e suas posteriores alterações. Em casos de dúvidas ou esclarecimentos sobre o conteúdo deste Manual ou sobre a aplicação do mesmo em relação a algum assunto específico, o departamento de compliance deverá ser consultado.
O descumprimento de alguma regra desta política será considerado como falta Grave, conforme disposto no Código de Ética e Conduta do BR.Offices ou de acordo com análise de decisão do Grupo.