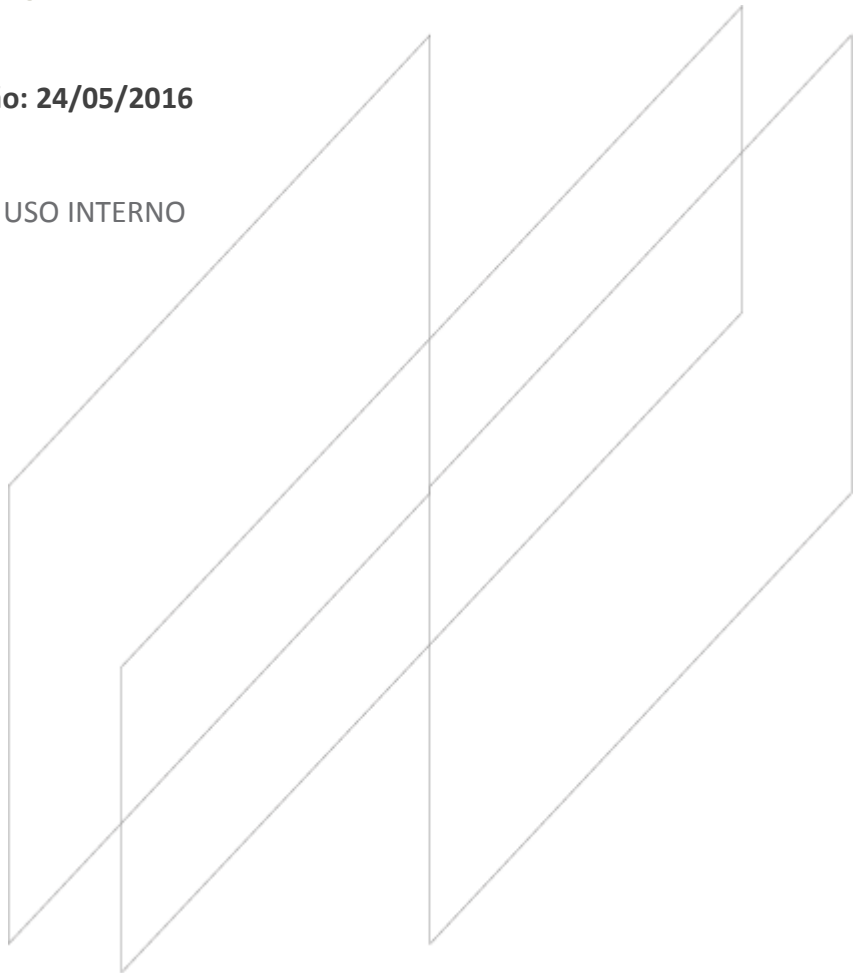
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Última atualização: 24/05/2016

EXCLUSIVO PARA USO INTERNO



Produzido pelas áreas de Compliance e TI-Infra.
Aprovado e revisado pelo Comitê de Compliance.

A reprodução e a distribuição desta Política fora do MODAL sem a devida autorização é terminantemente proibida e constitui uma violação da política de controles internos.

ÍNDICE

I. OBJETIVO

A Política de Segurança da Informação ("Política") visa preservar a confidencialidade, integridade e disponibilidade das informações utilizadas pelas empresas do Grupo *MODAL* (MODAL) no desempenho de suas atividades, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte, bem como estabelecer regras para acesso físico às instalações do MODAL.

II. ABRANGÊNCIA

Esta política abrange todos os Colaboradores e Visitantes que possuam acesso à rede Modal, à informações confidenciais, aos equipamentos computacionais ou ambientes controlados que necessitem de um *login* ou cartão de acesso, para que lhe sejam disponibilizados tais informações.

Terão acesso às Informações Confidenciais e ambientes controlados do *MODAL*, dentro dos limites definidos, os Colaboradores que concordarem com a política registrando o aceite através da assinatura do TERMO DE COMPROMISSO apresentado quando de sua admissão no Modal. Este termo determina a adesão do profissional a todas as políticas e normas internas, incluindo esta política.

O uso indevido dos recursos, em desacordo com a política poderá implicar em advertência, suspensão e demissão a critério da direção da empresa, conforme previsto na Matriz de Penalidades.

III. CONCEITOS

Para efeitos da presente política, considera-se:

Rede Modal: Abrange todos os sistemas, diretórios e Intranet disponibilizados aos Colaboradores do *MODAL*, conforme perfil de acesso definido.

Software: São todos os programas instalados nos computadores, os quais são disponibilizados pela equipe de TI INFRA para o exercício de sua função.

Homologação: Verificação pela equipe de TI INFRA quanto à compatibilidade técnica do software e aplicativos em relação ao parque tecnológico. Confirmação pelo usuário final do sistema do adequado funcionamento das funcionalidades previstas no quando da implantação ou da atualização de versão do mesmo.

Ambiente Lógico: ambiente controlado, eletrônico, onde circulam e são armazenadas Informações Confidenciais, softwares e sistemas.

Ambiente físico: dependências físicas das sociedades que integram o *MODAL*.

Usuário: Colaborador ou Colaboradores que detenham acesso aos ambientes físico e lógico das sociedades do *MODAL* para o desempenho de suas atividades.

Equipamentos Computacionais: São todos os equipamentos de propriedade das sociedades componente do *MODAL* disponibilizados ao uso dos colaboradores, incluindo, mas não se limitando, aos *desktops*, *notebooks*, impressoras, equipamentos de vídeo conferências e digitalizadores.

Informações Confidenciais: São consideradas informações confidenciais, para os fins desta Política, quaisquer informações consideradas não disponíveis ao público ou reservadas, dados, especificações técnicas, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, software e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pelo *MODAL* em decorrência do desempenho de suas atividades.

Colaborador ou Colaboradores: todos os associados, prestadores de serviço e quaisquer prepostos das sociedades que compõem o *MODAL*.

Associados: todos os profissionais que mantenham vínculo empregatício ou participação social em quaisquer das sociedades do *MODAL*.

Prestadores de serviços: pessoa jurídica ou física que mantenha contrato de prestação de serviço, ou tenha celebrado instrumento afim com quaisquer das sociedades do *MODAL*.

Visitante: todo indivíduo que não mantenha qualquer sorte de vínculo formal com as sociedades do *MODAL*, enfim, todos aqueles que não se enquadram na definição de Colaborador, conforme acima.

IV. RESPONSABILIDADES

MODAL

- Inclusão no planejamento orçamentário anual o valor de investimento em recursos computacionais, incluindo aquisição e renovação de equipamentos e softwares;
- Fornecer capacidade suficiente para realização dos Backups referentes aos processos e atividades da empresa;
- Fornecer espaço suficiente no SERVIDOR DE ARQUIVOS para armazenamento seguro de arquivos que contenham informações referentes aos processos e atividades da empresa.

EQUIPE DE TI

- Administrar e atualizar a capacidade do Backup;
- Administrar e atualizar a capacidade de armazenamento;
- Auxiliar os departamentos com fornecimento de informação técnica dos recursos em uso;
- Realizar de segunda a sexta-feira o backup das caixas postais armazenadas no servidor Exchange;
- Execução das rotinas de backup e restauração de dados dos servidores.

GESTORES DE DEPARTAMENTO

- Indicação de suas necessidades de recursos de TI;

- Utilização dos recursos de TI de acordo com o Código de Conduta do MODAL;
- Utilização da ferramenta de Correio Eletrônico para uso profissional;
- Orientação às suas equipes quanto a aplicação das normas previstas nesta política.

V. POLÍTICA DE CONFIDENCIALIDADE

Neste item são definidas como serão tratadas as informações institucionais, forma de uso, possibilidade ou não de disponibilização ao ambiente externo ou a terceiros. Assim, sempre que houver a necessidade de utilização de informações de conteúdo institucional, é necessário atentar-se para as determinações abaixo descritas:

V.1 PROPRIEDADE DAS INFORMAÇÕES E SOFTWARE

Os dados e informações criados nos Recursos Computacionais do MODAL são de sua propriedade e devem ser utilizados pelos Colaboradores, Prestadores de Serviços e Consultores, exclusivamente, no exercício de suas atividades junto à empresa.

Os softwares adquiridos no mercado ou desenvolvidos internamente pertencem exclusivamente ao MODAL, bem como todos os direitos relativos a todas as invenções, inovações tecnológicas, elaboradas e/ou desenvolvidas pelos Colaboradores, durante a vigência da relação de emprego ou contrato, ou quando forem utilizados recursos, dados, meios, materiais, instalações, equipamentos, informações tecnológicas e segredos comerciais, pertencentes ao MODAL, sendo vedada a cópia ou disponibilização através de qualquer meio (eletrônico ou físico) para ambiente externo ao MODAL.

Toda estrutura mantida pelo MODAL, composta pela rede, telefonia, correio eletrônico, internet e outros meios de comunicação, são instrumentos de trabalho de sua propriedade que o mesmo disponibiliza aos Associados a fim de tornar suas tarefas mais eficientes. Da mesma forma, todos os documentos, estejam eles em forma impressa ou eletrônica, ou que circulem por estes meios, também são de propriedade do MODAL e todos os Associados devem envidar esforços para protegê-los do uso indevido. É proibido o uso destes documentos fora do MODAL cujo objetivo não seja atender, exclusivamente, aos interesses da instituição, e, ainda assim, sua retirada ou envio somente poderá ser efetuado com autorização do sócio da área demandante e do sócio responsável por TI. Sua retirada ou envio com qualquer outra finalidade constitui violação a esta política. A sua transmissão via correio eletrônico, fax ou outro meio, deverá ser feita com o máximo de atenção e seguindo as regras de segurança e confidencialidade constantes nesta Política e no Código de Ética. Os documentos alterados fora do MODAL devem ter seus arquivos, manuais ou na rede, atualizados imediatamente.

Lembramos que todas as ações realizadas nos computadores corporativos tem os *logs* (registro de eventos) registrados, podendo ser a qualquer tempo auditados e monitorados, com o objetivo de garantir a aplicação desta Política.

V.2 CLASSIFICAÇÃO DA INFORMAÇÃO

As informações que transitam pelo MODAL são, para fins desta Política, classificadas em quatro padrões distintos, a saber:

INFORMAÇÕES PÚBLICAS: Aquelas destinadas a disseminação fora do MODAL. Possuem caráter informativo geral e são direcionadas a clientes ou investidores. Exemplos: material de marketing, *clipping information*, registros regulamentares e da Comissão de Valores Mobiliários.

INFORMAÇÕES INTERNAS: São aquelas destinadas ao uso dentro do MODAL. A divulgação de informações desta natureza, ainda que não autorizada, não afetaria significativamente o MODAL ou seus clientes e associados. Essas informações não exigem proteções especiais salvo aquelas entendidas como mínimas para impedir a divulgação externa não intencional.

INFORMAÇÕES CONFIDENCIAIS: Também destinam-se a uso interno do MODAL. Entretanto, diferem das informações de natureza interna à medida que sua extensão em uma eventual divulgação, poderia afetar significativamente os negócios do MODAL, seus clientes, investidores e associados. Exemplos: registros de funcionários, planos salariais, informações sobre clientes, sejam elas genéricas ou específicas, classificação de crédito, saldos de contas-correntes. Sua divulgação é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, CVM e Receita Federal, por exemplo), situação na qual deverá ser prestada por uma das seguintes pessoas: Contador, Controller, Auditor Interno, Advogado ou um dos sócios.

INFORMAÇÕES ALTAMENTE RESTRITAS: Correspondem a mais alta classificação de segurança para as informações que transitam no MODAL. Destina-se às informações cuja divulgação não autorizada, provavelmente provocaria danos substanciais, constrangimentos ou penalidades ao MODAL, seus clientes, investidores ou associados. As pessoas designadas para o trato e uso de tais informações, têm a responsabilidade de garantir que elas sejam devidamente protegidas e seguramente armazenadas quando não estiverem em uso. Exemplos: informação antecipada e não autorizada de novos produtos ou serviços, informações de fusões, aquisições ou outras atividades do mercado de capitais não disponíveis ao público em geral.

Em função desta categorização, é possível, quando do envio de informações sensíveis, a utilização de funcionalidade do Outlook, que permite classificar arquivos e mensagens conforme sua criticidade, que devem ser considerados sempre quando o mesmo for disponibilizado ou encaminhado para terceiros.

Sempre que forem trocadas informações sensíveis, orienta-se a utilização de senhas, sistemas de criptografia ou EDI (*Eletronic Data Interchange*) minimizando riscos de que informações sensíveis do MODAL sejam acessadas por terceiros.

VI. POLÍTICA DE PRIVACIDADE

VI.1 CORRESPONDÊNCIA ELETRÔNICA

Tal como telefone, fax, carta e outros documentos, o e-mail também é forma de comunicação de uso do *MODAL*, cujo objetivo é tornar suas atividades mais rápidas e fáceis. O e-mail também caracteriza um compromisso com terceiros, sejam eles clientes ou prestadores de serviço, e equivale aos papéis timbrados do *MODAL*, portanto, o uso desta ferramenta deve ser feita de forma cautelosa, profissional e com linguagem adequada.

O MODAL utiliza um padrão de *auto-signature* em cada correspondência eletrônica enviada, visando a mesma proteção legal das mensagens enviadas por fax. É expressamente proibida a alteração ou exclusão deste padrão de *auto-signature*.

Como se trata de ferramenta de trabalho de propriedade do *MODAL*, as empresas do grupo se reservam ao direito de rastrear, monitorar, gravar e inspecionar quaisquer informações transmitidas através de correspondência eletrônica, sem prévio aviso, com objetivo de evitar riscos decorrentes de ataques externos e do mau uso da ferramenta. Os Colaboradores, com a aceitação dos termos e condições desta Política, autorizam o *MODAL* a acessar as informações transmitidas e recebidas em suas através de suas contas de e-mail, ficando cientes de que o uso indevido ou não autorizado os sujeitará a punições. Todos os e-mails enviados, principalmente aqueles com arquivos anexados, devem ser rigorosamente checados e enviados com o máximo cuidado com relação ao destinatário para evitar que informações confidenciais ou de uso restrito se extraviem.

Com relação ao uso do e-mail, algumas práticas são proibidas. São elas:

i) Assediar ou perturbar outrem seja através de linguagem inadequada, alta frequência de mensagens ou excessivo tamanho de arquivos;
ii) Enviar quantidade excessiva de mensagens de e-mail em lote ("*junk mail*" ou "*spam*") ou e-mails mal-intencionados ("*mail bombing*") que, de acordo com a capacidade técnica da rede, seja prejudicial ou sobrecarregue intencionalmente usuários, site, servidor, etc;
iii) Reenviar ou, de qualquer forma, propagar mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens; e
iv) Cadastrar em sites de compras e entretenimentos o e-mail corporativo como contato.

O MODAL adota o *software* Mail Marshall, através do qual realiza o filtro para verificação de mensagens recebidas e enviadas por seus Associados, com o intuito de minimizar os riscos de ataques externos (cavalos de Tróia e vírus), que conteúdos não autorizados ou ilegais possam chegar a sua rede ou que Informações Confidenciais sejam indevidamente encaminhadas a terceiros. Os e-mails retidos no filtro classificados como de baixo risco, serão armazenados em uma fila que poderá ser acessada pelos Associados a qualquer momento através da Intranet da Corretora e efetuar a liberação. Anexos como arquivos compactados, executáveis e outros que configurem possíveis ameaças não entrarão na fila do Associado.

O MODAL mantém ainda um sistema de manutenção histórica dos e-mails, o BARRACUDA, que realiza a gravação dos mesmos quando da sua entrada no Exchange. Este sistema permite a recuperação de mensagens e tem como objetivo a melhor administração das caixas de e-mail. Em função do BARRACUDA é possível aos usuários excluírem e-mails de sua caixa postal sem risco de perda definitiva do arquivo. Orienta-se que as caixas postais sejam limpas no mínimo mensalmente, evitando o consumo de memória do servidor de e-mails.

VI.2 WEBMAIL

É vedada a utilização de webmail, mesmo que disponibilizado pelo MODAL. Os acessos antigos mantidos pelos profissionais deverão ser desabilitados após a obtenção de acesso remoto via *Token*, ou quando elegível, via BlackBerry (consultar política específica de liberação do BlackBerry) conforme detalhado no item a seguir (Internet).

Desta forma, novos acessos ao e-mail corporativo de forma remota só serão disponibilizados pela disponibilização do *Token*.

VI.3 GRAVAÇÃO TELEFÔNICA

Em função da natureza das operações realizadas pelo Modal, os ramais das áreas relacionadas abaixo estão ligados a sistema de gravação de voz. Tais gravações permitem a solução de eventuais conflitos que surjam nas negociações realizadas pelo Modal e suas contrapartes, bem como possibilita a identificação de situações de não conformidades.

Estas gravações são verificadas periodicamente pelo Compliance e a escuta por qualquer funcionário só poderá ser realizada com a aprovação desta área ou seus Diretores.

As áreas que mantem sistemas de gravação ativos são:
Corporate
Asset
Private Equity
Custódia
Controle de Fundos
Mesa de Operações
Distribuição
Ouvidoria
Corretora

VI.4 UTILIZAÇÃO DE TELEFONES CELULARES

Fica vedada a utilização de telefones celulares pelas áreas definidas abaixo. Tal restrição advém de previsão na regulamentação em vigor e garante que todas as comunicações com clientes passam pelo processo de gravação, seja ela de voz ou de mensagem.

Mesa de Corretora
Sales & Trading
Asset

VI.5 – UTILIZAÇÃO DE FILE TRANSFER PROTOCOL (FTP)

As trocas de arquivos e informações devem ser realizadas através de sistema de transferência aprovadas e de controle do TI-Infra, que utilizará, preferencialmente, o File Transfer Protocol (FTP). Essa ferramenta poderá ser utilizada pelos usuários, solicitando através de E-mail para TI-Infra e Compliance, ou ainda abertura de chamado pelo Help Desk. A autorização da transferência de informações e arquivos está condicionada à existência de um Non Disclosure Agreement (NDA) entre as partes.

Para o recebimento de arquivos não é necessário a existência e assinatura de NDA.

VII. POLÍTICA DE SENHAS E DIREITO DE ACESSO

VII.1 SENHAS

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos. Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso. Cabe aos usuários a memorização de suas senhas, sendo sugerida a não utilização de códigos comuns, tais como: o próprio nome, data de nascimento, nomes de parentes, números telefônicos, palavras existentes no dicionário e números sequenciais, etc.

Por procedimento de segurança, o usuário que proceder a 03 (três) tentativas seguidas de acesso com senha inválida terá sua conta bloqueada, e deverá contatar o Departamento de TI para que realizem o desbloqueio da mesma, tendo em vista que tal departamento é responsável pelo gerenciamento das senhas.

Com relação aos parâmetros para criação da senha de acesso, todo usuário deverá utilizar senha composta de no mínimo 6 dígitos, entre letras (utilizar maiúsculas e minúsculas), números e caracteres especiais.

O prazo máximo de duração da senha de acesso é de 45 (quarenta e cinco) dias contados de sua criação/alteração, sendo que, 15 dias antes do fim do referido período o sistema notificará o usuário para acerca da expiração da senha.

O histórico mínimo de senhas utilizadas é de 6 senhas.

Mecanismos para elaboração de senhas:

- Utilize preferencialmente senhas distintas para usos distintos, evitando repetir senhas de uso pessoal para acessos corporativos.
- Uma senha boa, bem elaborada, é aquela que é difícil de ser descoberta (forte) e fácil de ser lembrada. Desta forma, evite o uso de dados pessoais, sequencias de teclado, palavras que fazem parte de listas publicamente conhecidas (times de futebol), por exemplo.
- Selecione caracteres de uma frase: “Eu trabalho no Banco MODAL há 3 anos e 1 mês”: EtBMh3a.1m
- Utilize uma frase longa, como parte de uma música, por exemplo: “Ninguém segura a juventude do Brasil”
- Faça substituição de caracteres semelhantes: “Astro-rei” por “A5tr0-re1”

VII.2 ACESSOS A SISTEMAS

O MODAL utiliza em sua plataforma de softwares sistemas desenvolvidos internamente (SIN e SMART) e adquiridos de terceiros.

Quando da admissão ou transferência de Associado a área de RH emite um *Check list* de admissão ou de transferência, para o qual cada área deve tomar uma ação específica. Dessa forma, para os acessos a sistemas, o novo funcionário recebe apenas acesso ao sistema SMART, em conformidade com o perfil espelho.

Para os demais sistemas, o profissional deverá, obrigatoriamente, abrir chamado através do Help Desk solicitando os acessos necessários. Sendo analisado e aprovado pelo Compliance e executado pelo TI-DBA.

O acesso aos sistemas próprios se dá através da solicitação por parte dos usuários através de registro de chamado pelo Help Desk ou envio de e-mail. Esta informação é passada ao Compliance que analisa junto ao "Gestor" do sistema a possibilidade de acesso as funcionalidades e ainda o tipo de acesso passível para a área e cargo do usuário, garantindo a limitação de acesso a informações críticas. Após as devidas aprovações, TI-DBA executa a liberação do acesso no respectivo sistema.

Para o SMART todos os acessos são executados pelo Compliance diretamente no sistema e para o SIN, após a aprovação do Compliance, é efetuada a execução do acesso por TI-DBA.

É possível o uso de usuários genéricos que podem ser utilizados como usuários de serviço para permitir interface de dados entre os diversos sistemas utilizados ou ainda usuários administrativos. O primeiro tipo serve para ser configurável nos sistemas para possibilitar a integração de informações. O segundo tipo será de uso compartilhado do TI-DBA, sendo ambos os tipos de responsabilidade do profissional sênior, podendo ser transferido ao seu substituto imediato. Esses usuários respondem objetivamente por qualquer violação aos dados e deverão assinar termo de responsabilidade específico.

VII.3. ACESSO A DIRETÓRIOS

Todos os associados quando admitidos ou transferidos de área receberão um perfil básico, o qual dará acesso ao G:/Depto da área do associado, ao J:/Users do usuário, ao grupo de e-mail da área e ao grupo de e-mail TODOS. Este procedimento é realizado a partir do recebimento do *Check list* de admissão ou transferência, emitido pelo RH e implementado pela área de TI-Redes.

Qualquer acesso específico do associado que seja necessário para o andamento de suas atividades deverão ser solicitados através da abertura de chamado no Help Desk na Intranet, cuja solicitação será analisada pelo Compliance, que junto ao Gestor imediato do profissional deliberará sobre a aprovação ou não do acesso. É necessário que o usuário no momento da abertura do chamado informe se seu acesso àquela partição da rede será para consulta a informações (leitura) ou para edição do conteúdo (escrita). Esta condição também será analisada pelo Compliance. Caso o acesso seja aprovado, TI-Redes executará o procedimento de liberação ao acesso.

VII.4. ACESSO AO USB

Por motivos de segurança todos os drives A:\ e entradas USB dos computadores do MODAL estão desabilitados pela aplicação SEP (antivírus).

O acesso à entrada USB fica permitido apenas para os Sócios, TI e Comunicação, os demais usuários, quando necessitarem gravar arquivos neste *gadget* para fins profissionais, deverão formalizar sua necessidade através de e-mail para TI-Help Desk, Sócio Responsável pela área e Compliance, com a justificativa de gravação do arquivo, bem como seu conteúdo. O Sócio e o Compliance deverão aprovar esta gravação, que poderão verificar o conteúdo do material gravado antes de liberar para o uso por parte do associado.

VII.5. ACESSOA À REDE VIA WI-FI (WIRELESS FIDELITY)

O acesso à rede interna via Wi-Fi só é permitida para os Sócios, TI- HelpDesk, TI-Redes e para visitantes externos que utilizarão as salas de reunião para apresentações ou auditorias.

Este acesso é vedado para os demais associados.

VII.6. ACESSO À REDE INTERNA ATRAVÉS DE CONEXÃO REMOTA

O MODAL disponibiliza ainda acesso ao ambiente interno através de conexão remota segura, para a qual é necessária a utilização de um *Token* para emissão de chave de acesso. Todos os usuários que eventualmente tenham necessidade de utilizar a rede interna deverão solicitar a aquisição de um *Token*, que deverá ser autorizado pelo Sócio Responsável.

O *Token* deverá ser utilizado com o máximo de cuidado em função da possibilidade de acesso ao ambiente interno do MODAL, além de envolver custo por conta da aquisição de licença específica para esse fim.

VII.7 ACESSO AOS AMBIENTES

O MODAL, pela natureza de suas operações, deve manter ambientes isolados para a manutenção de suas operações e negócios, por onde transitam informações sobre operações, posições e estratégias que só podem ser de conhecimento das áreas responsáveis pelo negócio e seu processamento. A disponibilização indevida de tais informações ou permissão de acesso ao ambiente segregado por pessoa não autorizada é **terminantemente proibida**.

As áreas que mantém acesso controlado aos seus ambientes são:

- Asset Management
- Private Equity
- Sales & Trading
- Corretora
- Serviços Qualificados
- CPD

O Compliance realizará verificações periódicas em relatórios de acesso aos ambientes descritos acima, podendo a qualquer tempo alterar os níveis de acesso em função de identificação de não conformidade.

O acesso de visitantes (inclusive ex-funcionários) no ambiente operacional do Modal só poderá ocorrer com acompanhamento de funcionário, sendo vedada a circulação de terceiros sem autorização específica para isso.

VII.8 INTERNET

O acesso à Internet é permitido a todos os Associados usuários de computador, com o objetivo de facilitar suas tarefas. Assim como qualquer outro material de trabalho, as páginas da Internet também devem ser usadas somente para fins profissionais.

Para uma utilização eficiente e produtiva algumas regras devem ser obedecidas:

- É proibido o acesso a sites ilegais ou não autorizados, tais como os relacionados a sexo, pornografia, pirataria, atividades de hacker e quaisquer outras atividades ilegais. Estes exemplos não esgotam a lista de sites proibidos, portanto quaisquer dúvidas devem ser levadas ao conhecimento da área de TI - HelpDesk.
- É terminantemente proibida a utilização de webmail (UOL, IG, Gmail, etc.) através da rede do MODAL;
- Fica proibido também o download de arquivos e programas não autorizados ou sem revisão e aprovação da TI - Infra.
- É vedado também o acesso à sites de Corretoras, com o objetivo de efetuar operações de renda variável.

A intenção desta política é evitar que vírus, cavalos de Tróia e outros programas indevidos, não licenciados e nocivos apareçam no ambiente de computação do MODAL.

Os acessos à Internet são controlados por um servidor de Proxy, que atribui uma autenticação a cada conexão feita pelo Associado, gerando *log's* de acesso aos sites visitados. Esses *log's* dão origem a relatórios que são repassados aos Sócios responsáveis de cada área para análise.

Aliada a essa funcionalidade temos o controle de acesso aos sites não permitidos relatados anteriormente, impedindo que os mesmos sejam acessados. Quaisquer atividades que contrariem as regras de acesso à Internet ficarão sujeitas à penalidade.

Quando observado por um associado a necessidade de acessar um determinado site que está previamente bloqueado, para fins profissionais, é possível solicitar o acesso a ele abrindo um chamando no Help Desk na Intranet, informando endereço do site, justificativa para acessá-lo e período que precisa acessar.

O Compliance analisará a solicitação, verificando junto ao Gestor imediato a real necessidade de acesso ao site, em caso de aprovação, o Compliance informará no chamado os seguintes dados:

Site liberado para todos os usuários da instituição?
Site liberado para todos os usuários do setor?
Site liberado para o solicitante?
Data de revogação do acesso

Estas informações são essenciais para a adequada administração dos acessos temporários aos sites bloqueados.

VII.9 PROCEDIMENTOS DE RETIRADA DE ACESSO

Quando um Associado é desligado do MODAL, ele perde imediatamente o direito de acesso aos diversos ambientes de rede, serviço de e-mail externo e internet. Este procedimento é iniciado quando do envio de *Check List* de desligamento, quando as áreas responsáveis pelos acessos deverão providenciar o cancelamento das credenciais de acesso de profissional.

No caso de transferências internas, os direitos de acesso originais são retirados na data prevista no *Check List* de transferência. Os novos acessos seguem o perfil básico, sendo necessária a abertura de chamado para liberação dos demais acessos a sistemas e ambientes da rede necessários ao desenvolvimento das atividades na nova área. É possível que por um

período pré-determinado, o profissional utilize informações e arquivos de ambas as áreas, em função da necessidade das áreas. Caso isso seja necessário, o profissional deve solicitar, através de abertura de chamado, a manutenção dos acessos antigos ou liberação dos novos acessos, com a justificativa sobre a manutenção de ambos os acessos, bem como o prazo máximo de manutenção deles, não podendo ultrapassar 30 dias.

Os profissionais demissionários terão, em caso de solicitação por parte de seu gestor imediato, os e-mails monitorados através de cópia das mensagens enviadas para a caixa postal do gestor, além de monitoramento semanal dos sites visitados pelo associado até o desligamento efetivo do profissional.

Os trabalhos desenvolvidos ou elaborados pelo Associado pertencem exclusivamente ao MODAL, não cabendo ao associado o direito de retirá-lo ou copiá-lo quando de seu desligamento, não sendo permitida a gravação de arquivos em qualquer mídia sem a devida autorização por parte do Compliance.

VIII. POLÍTICA DE BACKUP

O backup dos diretórios de rede é realizado diariamente através de processo automatizado, em fita, sendo encaminhados para armazenamento junto a prestador de serviço de guarda especializado, devidamente contratado para este fim, no dia seguinte (D+1).

G:\Depto - *Snapshot* executado a cada duas horas (8h, 10h, 12h, 14h, 16h, 18h, 20h, 22h), mantendo as últimas 8 cópias, a 0h é executado outro *Snapshot* e este é armazenado por 30 dias, além destes existe outro *Snapshot*, semanal, executado aos domingos e este é mantido por 5 semanas.

J:\Users - *Snapshot* executado a cada duas horas (8h, 10h, 12h, 14h, 16h, 18h, 20h, 22h), mantendo as últimas 8 cópias, a 0h é executado um outro *Snapshot* e este é armazenado por 7 dias, além destes existe um outro *Snapshot*, semanal, executado aos domingos e este é mantido por 4 semanas.

H:\SISTEMAS - *Snapshot* executado a cada duas horas (8h, 10h, 12h, 14h, 16h, 18h, 20h, 22h), mantendo as últimas 8 cópias, a 0h é executado um outro *Snapshot* e este é armazenado por 2 dias, além destes existe um outro *Snapshot*, semanal, executado aos domingos e este é mantido por 2 semanas.

I:\ CORREIO - *Snapshot* executado 1 vez por dia, executado a 0h.

O Backup do Exchange/emails também é realizado diariamente. A retenção de emails deletados é de 07 (sete) dias.

IX. POLÍTICA DE USO ACEITÁVEL

IX.1 ESTRUTURA DA REDE

A rede do MODAL é composta por servidores de arquivos, de banco de dados, aplicações e e-mail e está organizada da seguinte forma:

G:\Depto – Diretório onde devem ser armazenados todos os arquivos de trabalho (planilhas, documentos e apresentações) comuns ao departamento ao qual o Associado pertence.

J:\Users – Diretório para armazenagem de arquivos que não sejam comuns ao departamento ou aqueles que, por estarem em fase de desenvolvimento, ainda não foram alocados no G:\Depto.

I:\Correio – Diretório de uso temporário para transferência de arquivos aos quais todos os Associados têm acesso. Não deve ser utilizado para armazenagem ou transferência de arquivos confidenciais ou de uso restrito, em virtude do mesmo ser de acesso público. O conteúdo deste diretório é totalmente apagado ao final do último dia útil de cada semana.

H:\Sistemas – Diretório de repositório dos arquivos de sistemas homologados pela área de TI para utilização em rede. O acesso a esse diretório é concedido conforme o perfil dos associados. Tal perfil determina quais os sistemas o associado possui acesso.

IX.2 SOFTWARE E COMPUTADORES

Para mantermos o ambiente lógico, todos os softwares/aplicações operacionais devem ser homologados pelos usuários das áreas envolvidas, que devem verificar os impactos das novas versões nos procedimentos, resultados e impostos.

Aquisição: A aquisição de softwares ocorrerá conforme planejamento orçamentário, com base na homologação técnica por parte da equipe de TI, após validação das necessidades de uso pela diretoria da empresa.

Instalação: Somente a equipe de TI INFRA está autorizada a realizar instalação de qualquer tipo de software, seja este um sistema ou um aplicativo simples, principalmente aqueles obtidos gratuitamente e/ou baixados da internet.

Licença de Uso: Somente poderão ser instalados e utilizados softwares devidamente licenciados para uso do MODAL. Não é permitido instalar softwares pessoais, emprestados, de terceiros, que não sejam devidamente licenciados para uso do MODAL pelo fabricante do produto.

Auditoria: Poderá ser utilizada pela equipe de TI INFRA uma ferramenta automatizada para auditoria de softwares instalados nos computadores.

Marcas e Modelos: Utilização de equipamentos padronizados pela equipe de TI INFRA.

Distribuição: Os computadores são disponibilizados conforme necessidades de uso de cada colaborador, com base nos softwares destinados à automação de sua área. As impressoras ficarão distribuídas em centros de impressão, localizados em pontos que melhor atendam a maioria dos colaboradores e não estejam em áreas que impliquem em risco à segurança do patrimônio.

Propriedade: Os softwares, incluindo os desenvolvidos internamente, e recursos computacionais diversos pertencem exclusivamente ao MODAL, bem como todos os direitos

relativos a todas as invenções, inovações tecnológicas e criações intelectuais elaboradas e desenvolvidas pelos Colaboradores, Prestadores de Serviços e Consultores, durante a vigência da relação de emprego ou relação contratual.

IX.3 SISTEMAS INTERNOS E APLICATIVOS

O MODAL somente utiliza softwares aprovados e licenciados na execução de suas tarefas, não sendo permitido o uso pelos Associados de softwares que contrariem esta norma.

O uso de software não licenciado é crime previsto na Lei 9.609 de 19 de fevereiro de 1998. Além disso, existe um risco considerável na utilização de quaisquer softwares externos ao ambiente, destes possuírem vírus ou outras ameaças de segurança escondidas.

A instalação de softwares autorizados e cópias de arquivos para uso fora do MODAL, *em pen drives*, cds, USB ou em outras mídias, deve ser autorizadas pelo Sócio Responsável pela área, bem como pelo Compliance. É proibida a execução destas tarefas por Associado que não pertença à área de TI Infraestrutura.

IX.4 VÍRUS

A qualquer indício de existência de vírus, o Associado deve interromper suas tarefas e comunicá-lo imediatamente à TI Infraestrutura, que executará os procedimentos para a erradicação de vírus determinados na Política de Segurança. Mesmo em caso de falta de notificação por parte do Associado, o SEP (anti-vírus) envia um e-mail de alerta para a área de TI passando todos os detalhes do fato ocorrido, facilitando uma ação rápida no intuito de evitar a propagação do problema.

Os esforços individuais e isolados dos usuários para acabar com os vírus podem contribuir para provocar danos ainda maiores, pois, em geral, estes usuários não estão capacitados para esta atividade.

O uso de softwares freeware ou shareware e arquivos em outras mídias constituem formas muito comuns de transferência de vírus para os computadores, portanto, sua utilização sem a prévia autorização da TI Infraestrutura é terminantemente proibida.

Além dos programas que protegem a rede, todos os computadores possuem software de verificação de integridade (agente do antivírus), que detecta alterações nos arquivos de configuração e nos softwares e alertam ao usuário da possibilidade de existência de vírus. Isso ocorrendo, o mesmo deve notificar a TI - Infra imediatamente.

Todos os equipamentos utilizados para gravação de informações em computadores que ligados à Rede Modal deverão ser apresentados ao Departamento de TI para verificação e certificação da inexistência de vírus que possam ocasionar danos estrutura da Rede Modal.

IX.5 HARDWARES E SOFTWARES PESSOAIS

Equipamentos de utilização pessoais, tais como Blackberry, Notebook ou Aparelho de Telefone Celular, são cedidos aos Associados para que desenvolvam suas atividades profissionais, sendo obrigatória a assinatura de um termo assumindo toda a responsabilidade pelos mesmos e pelos softwares neles instalados. As regras de utilização destes equipamentos encontram-se previstas nas políticas específicas.

X. NOTIFICAÇÃO DE INCIDENTES E ABUSOS

Um incidente de segurança pode ser definido como qualquer evento adverso, confirmado ou suspeito, relacionado à segurança de sistemas e redes. Alguns exemplos são: tentativa de uso ou acesso não autorizado a sistemas e dados, tentativa de tornar serviços indisponíveis, desrespeito à política de segurança.

É responsabilidade dos Associados notificar a área de Risco Operacional ou Compliance, sempre que se deparar com uma atitude que considere abusiva ou com um incidente de segurança para que sejam tomadas as devidas ações, minimizando os impactos da ocorrência.

XI. PLANO DE CONTINGÊNCIA E CONTINUIDADE DE NEGÓCIOS

Está disponível na Intranet do MODAL para observação de todos os associados o Manual de Contingência e Continuidade de Negócios, no qual estão abrangidas as contingências de Infraestrutura física, contingências de Pessoal e contingências de Infraestrutura tecnológica, a fim de estarem aptos a executar os procedimentos em situações de emergência. O referido plano é o conjunto de medidas preventivas e procedimentos de recuperação, para que o MODAL possa permanecer operando em bases contínuas.