MANUAL DE CONTROLES INTERNOS DE SEGURANÇA

30 / JUNHO / 2017

Manual de Controles Internos de Segurança			
Classificação	Tipo	Atualizado em	Dpto. responsável
Público	Manual	30/06/2017	*Compliance*

SUMÁRIO

1. INTRODUÇÃO

Este Manual de Controles Internos de Segurança (o "Manual de Segurança") especifica os controles internos aplicáveis à segurança e ao sigilo da informação, e à continuidade dos negócios das empresas do conglomerado da BRIDGE (a "BRIDGE"), com os seguintes objetivos:

- permitir que a BRIDGE atenda à regulamentação, legislação e autorregulação aplicáveis;
- garantir a devida identificação/autenticação e a adequada autorização dos usuários;
- garantir a confidencialidade, a integridade e a disponibilização das informações da BRIDGE nos termos das normas vigentes e padrões internos;
- manter o nível de segurança da organização em patamar definido como adequado pela BRIDGE;
- garantir que as diretrizes explicitadas neste Manual sejam praticadas por meio da implementação de controles que visam garantir a confidencialidade, a integridade e a disponibilidade das informações;
- prover a segurança necessária para realização de suas operações, ainda que em situações adversas.

A BRIDGE estabelece o presente Manual como um dos pilares de sua estratégia de segurança, que deve ser seguida e implementada para garantir que os Ativos sejam protegidos de acordo com a sua importância estratégica para a organização.O presente Manual foi elaborado e deve ser interpretado em consonância com os demais manuais e políticas da BRIDGE, e deve ser revisado e atualizado anualmente pela área de *Compliance*, com o apoio das demais áreas internas, principalmente Administrativa e de Tecnologia, a fim de incorporar medidas relacionadas a atividades e riscos novos ou anteriormente não abordados.

Estão sujeitos ao disposto no presente documento todos os colaboradores das empresas do conglomerado BRIDGE, no que a cada uma aplicável, sendo sua obrigação conhecer a versão mais recente do Manual na íntegra.

O presente Manual de Segurança está dividido em 03 (três) capítulos que cobrem, respectivamente, a segurança das informações (a "Política de Segurança das Informações"), o sigilo das informações (a "Política de Sigilo das Informações") e a continuidade dos negócios (o "Plano de Continuidade dos Negócios).

2. DEFINIÇÕES

Para o perfeito entendimento deste Manual, faz-se necessário estabelecer o significado de alguns termos aqui mencionados, a saber:

- **Antivírus*:*** programa que detecta e elimina vírus de computador.
- **Ativo**: todo equipamento, instalação, sistema e informações, bem como a quaisquer outros bens, tangíveis ou intangíveis, de propriedade ou administrados pela BRIDGE. Da mesma forma, se aplica a todas as plataformas de *hardware* e a todos

os sistemas operacionais e aplicativos utilizados. Aplica-se também a qualquer meio onde a informação possa ser armazenada, incluindo mídias magnéticas, discos ópticos, "nuvens" de armazenamento, informações impressas em papel e material de marketing. Os Ativos podem ser:

- ✓ **Ativo de informação**: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas, etc.
- ✓ **Ativo de *software***: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.
- ✓ **Ativo físico**: equipamentos computacionais (computadores, processadores, monitores, *laptops*, *modems*, etc.), equipamentos de comunicação (roteadores, *PABX*, telefones fixos, etc.), mídias (fitas e discos magnéticos, discos ópticos, etc.), outros equipamentos técnicos (*no-breaks*, aparelhos de ar-condicionado, etc.), mobília, acomodações, etc.

- ***Backup*:** cópia exata de um programa, disco ou arquivo de dados feita para fins de arquivamento ou para salvaguardar informações.
- **Cavalo de Tróia**: programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de *hackers*.
- **Colaboradores**: todas as pessoas que, de alguma forma, prestem serviços para a BRIDGE, sejam elas diretores, empregados, estagiários ou terceiros contratados. Todos devem dar cumprimento às regras definidas neste Manual de Controles Internos de Segurança.
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Controle de Acesso**: conjunto de restrições ao acesso às informações de um sistema aplicado pela equipe de segurança da informação.
- **Criptografia**: arte/ciência de utilizar matemática para tornar a informação segura, criando alto nível de confiança no meio eletrônico.
- **Direito de Acesso**: privilégio associado a um cargo, pessoa ou processo relativo ao acesso a um ativo.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que precisarem.
- ***Download***: transferência de arquivo de um computador para outro computador através da rede.
- **Ferramentas**: conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação.
- ***Handheld***: computadores que cabem na palma da mão (*palmtops*) e que possuem recursos para organização pessoal e comunicação móvel.
- **Incidente de Segurança**: qualquer ocorrência que comprometa ou ameace a integridade, autenticidade ou disponibilidade de qualquer ativo.

- **Integridade**: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
- ***Junk mail***: *e-mails* não solicitados por usuários não interessados em recebê-los.
- ***Log***: registro de transações ou atividades realizadas em sistema de computador.
- ***No-Break***: sistema com baterias que mantém o computador funcionando por determinado período.
- ***Peer-to-Peer***: rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdo e serviços à rede.
- **Política de Segurança**: conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos por sistemas de informação.
- **Proteção dos Ativos**: processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.
- **Segurança da informação**: preservação da confidencialidade, integridade e disponibilidade da informação.
- **Senha Fraca ou Óbvia**: senha que utiliza caracteres de fácil associação ao seu dono, que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome do usuário, nome de seus familiares, sequências numéricas simples, palavras com significado, dentre outras.
- **Spam**: *e-mail* não solicitado enviado a grande número de endereços eletrônicos que, geralmente, visa fazer propaganda de produtos e serviços.
- **Vírus**: programa construído para causar danos aos *softwares* do computador.

3. DEVERES E RESPONSABILIDADES

O presente Manual gera alguns deveres e responsabilidades para os usuários de informação da BRIDGE, conforme descritos abaixo.

3.1 Deveres de todos os colaboradores

- Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações.
- Proteger os Ativos da BRIDGE.
- Cumprir o disposto no presente Manual, sob pena de incorrer nas sanções disciplinares e legais cabíveis.
- Utilizar os Sistemas de Informações e os recursos relacionados somente para os fins previstos pela área de Tecnologia.

- Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação.

- Manter o caráter sigiloso da senha de acesso aos recursos e sistemas.

- Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso.

- Responder por todo e qualquer acesso aos recursos da BRIDGE, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação ou outro atributo para esse fim utilizado.

- Solicitar acesso a informações restritas somente quando houver real necessidade de acessar o recurso.

- Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente.

- Comunicar ao seu superior imediato e ao Departamento de *Compliance* o conhecimento de qualquer irregularidade ou desvio verificado no âmbito do presente Manual.

3.2 Responsabilidade dos gestores das áreas

- Gerenciar o cumprimento deste Manual, por parte de seus subordinados e de prestadores de serviço sob sua supervisão.

- Responsabilizar-se pelos Ativos de processamento e de informação detidos pela área sob sua supervisão.

- Identificar os desvios praticados e adotar as medidas corretivas apropriadas, reportando a situação ao Departamento de *Compliance*.

- Impedir o acesso de empregados demitidos aos Ativos.

- Controlar o acesso de empregados demissionários aos Ativos de informação.

- Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger todos os Ativos.

- Comunicar formal e tempestivamente ao *Compliance* e à área de Tecnologia quais são os empregados e prestadores de serviço sob sua supervisão que podem acessar as informações da BRIDGE.

- Comunicar formal e tempestivamente ao *Compliance* e à área de Tecnologia quais são os empregados demitidos ou transferidos, para que possam ser realizadas as respectivas exclusões no cadastro de usuários.

- Comunicar formal e tempestivamente ao *Compliance* e à área de Tecnologia quais são os usuários que estão respondendo a processos ou sindicâncias, para que possam ser efetuadas as respectivas inabilitações no cadastro de usuários.

- Comunicar formal e tempestivamente ao *Compliance* e à área de Tecnologia sobre movimentações de funcionários de sua equipe (desligamento,

contratação, transferência, etc.) para que possam ser realizadas a criação, modificação ou cancelamento das respectivas permissões de acesso.

3.3 Responsabilidades da equipe de Tecnologia

- Auxiliar os Departamentos Administrativo e de *Compliance* a elaborar e a manter atualizado o Plano de Contingência e Continuidade dos Negócios.
- Executar as regras de restrição, proteção, controle de acessos, e privilégios de usuários remotos e externos estabelecidas por este Manual e pela equipe de *Compliance*.
- Detectar, identificar, registrar e comunicar à chefia violações ou tentativas de acesso não autorizadas.
- Limitar ao período da contratação o prazo de validade das contas de prestadores de serviço.
- Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos.
- Excluir ou desabilitar as contas inativas.
- Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente de tais privilégios e desde que aprovado pela equipe de *Compliance*, mantendo-se o devido registro e controle.
- Garantir o cumprimento do procedimento de *Backup* para os servidores e Ativos.

3.4 Responsabilidades do Departamento de *Compliance*

- Estabelecer as regras de proteção e restrição dos ativos da BRIDGE.
- Estabelecer a política de privilégios de usuários remotos e externos.
- Revisar frequentemente as regras de proteção estabelecidas.
- Assessorar a BRIDGE na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os Ativos.
- Liderar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de segurança da informação aos regulamentos internos e externos da BRIDGE, ainda que auxiliado pela área de Tecnologia e demais áreas internas.
- Assegurar que as atividades da BRIDGE sejam desenvolvidas com base nos princípios estabelecidos em seus manuais/políticas internos e em consonância com a regulamentação, legislação e autorregulação aplicável.
- Dirimir ou ao menos mitigar a existência de conflitos de interesse relacionados ao desenvolvimento das atividades da BRIDGE, especialmente, para fins do disposto neste Manual.

- Garantir a segregação física e lógica das áreas de administração fiduciária e gestão de recursos da BRIDGE, por meio da restrição de acessos físicos e da criação de perfis de usuários para a rede interna.

- Elaborar e controlar a política de perfis e acessos físicos e lógicos da BRIDGE, inclusive quanto ao acesso a USB e CD Rom, criando os perfis de acesso e designando-os a cada colaborador de acordo com as atividades por ele desenvolvidas e com o cargo por ele ocupado.

- Atualizar a política de perfis e acessos, bem como solicitar à área de Tecnologia a liberação ou o bloqueio de perfis de acordo com as necessidades verificadas ou sob demanda dos colaboradores quando julgar pertinente.

- Aprovar a criação ou exclusão de usuários quando houver contratação ou demissão de efetivos ou de estagiários, sendo certo que os usuários novos devem ser cadastrados sem nenhum acesso, os quais devem ser solicitados posteriormente pelo respectivo gestor.

- Organizar treinamentos relacionados à segurança/proteção dos Ativos sempre que necessário.

Para permitir o cumprimento das obrigações acima expostas, a área de *Compliance* possui acesso irrestrito a todas as dependências da BRIDGE, inclusive salas com controle de acesso, bem como a toda a rede interna.

3.5 Responsabilidades do Departamento Jurídico

- Assessorar a BRIDGE na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os Ativos.

- Garantir que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula que preserve a segurança e confidencialidade das informações da BRIDGE.

- Garantir que a existência das diretrizes estabelecidas com base neste Manual e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos com terceiros, bem como nos contratos firmados com os colaboradores da BRIDGE, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito deste Manual.

3.6 Responsabilidades do Departamento Administrativo

- Executar as atividades de custódia e/ou administração dos meios de informação não informatizados da BRIDGE, tais como: fax, copiadoras, equipamentos de telefonia, de controle de acesso físico e de limpeza, arquivo, correio, mensageiros, impressoras, cabeamento, fragmentadores, salas de reunião, entre outros.

- Classificar os meios de informação não computadorizados que administra quanto à criticidade que representam, provendo as condições mínimas necessárias de continuidade, disponibilidade, integridade e legalidade desses meios, incluindo locais, serviços e equipamentos.

- Executar as ações para proteger os Ativos sob sua responsabilidade.

- Administrar os serviços de proteção, limpeza, transporte, armazenamento e destruição dos Ativos de informação.

- Informar às equipes de *Compliance* e de Tecnologia situações em que haja vulnerabilidade quanto à proteção dos Ativos.

- Assessorar as áreas de Tecnologia e *Compliance*, conforme aplicável, na criação, alteração e manutenção de novas políticas, normas, códigos ou regulamentos de segurança da informação.

- Participar, quando cabível, na apuração das responsabilidades e causas relacionadas a incidentes ou violações da segurança da informação.

- Divulgar e providenciar adesão dos novos colaboradores às normas, políticas, códigos e regulamentos internos da BRIDGE, no ato da admissão.

- Coordenar os procedimentos referentes ao Plano de Continuidade dos Negócios e orientar os colaboradores para sua correta execução, com o auxílio da área de *Compliance* e sob supervisão da Diretoria,

3.7 Responsabilidades dos Prestadores de Serviço

- Respeitar as obrigações previstas nos respectivos contratos de prestação de serviço, especialmente, para fins desse Manual, no que concerne à segurança e à confidencialidade da informação.

4. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação expressa a posição da organização sobre a segurança e define quais são os valores que devem orientar as atividades da BRIDGE e de seus colaboradores a fim de minimizar os riscos sobre seus Ativos.

Esta Política serve como um guia de melhores práticas definido pela BRIDGE em relação à segurança da informação e tem o propósito de oferecer uma base comum de atuação para ser usada por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros Ativos que fazem parte do cotidiano da BRIDGE. A BRIDGE tem como compromisso assegurar que as orientações definidas neste documento sejam seguidas por toda a organização.

A Política de Segurança da Informação tem como princípios assegurar a:

- Identificação: garantir que qualquer indivíduo seja identificado unívoca e inequivocamente;

- Autenticação: garantir que a identidade de cada pessoa ou recurso seja expressamente comprovada;

- Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos Ativos;

- Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles expressamente autorizados;

- Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas as informações estejam exatas e completas durante a sua criação, uso, guarda e destruição;

- Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo Ativos da BRIDGE, o usuário deve consultar esta Política para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja expressa e claramente permitida é proibida. Em caso de dúvida o usuário deve consultar o Departamento de *Compliance* e a equipe de Tecnologia para assegurar-se de que a atividade seja permitida. Cabe a estas áreas avaliar os riscos das atividades não previstas nas diretrizes de segurança formalizadas pela BRIDGE, levando ao conhecimento de comitê interno competente quando necessário.

4.1 Privacidade

Todos os Ativos pertencem à BRIDGE e, portanto, a BRIDGE tem direito de acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede, inclusive *e-mails* e conversas pelo *Skype* corporativo (mensagens eletrônicas), ou que se encontrem fisicamente no mobiliário da empresa, como, por exemplo, em mesas, estantes, gaveteiros, armários, etc. Dessa forma, ainda que o colaborador possa se utilizar da estrutura de tecnologia da empresa para algum uso particular não conflitante, tais informações podem ser acessadas pela BRIDGE mesmo sem o prévio consentimento do respectivo colaborador.

Com relação às ligações telefônicas, a BRIDGE se reserva o direito de monitorar as ligações e seus conteúdos, gravar registros das ligações e das respectivas conversas, bem como consultá-las sem prévio aviso ao colaborador.

Sem prejuízo do acima exposto, a BRIDGE garante que toda escuta a conversas telefônicas e consulta a dados depende do prévio consentimento da área de *Compliance*.

Por fim, vale ressaltar que os referidos registros de gravação serão arquivados por, no mínimo, 5 (cinco) anos.

4.2 Uso dos recursos de informática

4.2.1 Uso do *e-mail*

O uso do *e-mail* na BRIDGE está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. Com isso em vista, seguem as regras que devem ser observadas por todos os colaboradores quando da utilização desta ferramenta:

- O usuário é o único responsável pelo conteúdo das transmissões feitas através do *e-mail* a partir de sua senha ou conta.

- As mensagens de *e-mail* são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela.

- Não devem ser abertos arquivos ou executados programas anexados aos *e-mails* sem antes de verificá-los com um antivírus.

- Devem estar desligadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens.

- Não deve ser utilizado *e-mail* para fins ilegais.

- Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço.

- Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas não se limitando a, direitos de propriedade intelectual.

- Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis.

- O colaborador não pode obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço.

- Não devem ser utilizados os serviços de *e-mail* para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa que possa prejudicar o bom desempenho das atividades da BRIDGE e de seus Ativos.

- Não devem ser transmitidas mensagens não solicitadas, conhecidas como *spam* ou *junk mail*, correntes, *chain letters* ou distribuição em massa de mensagens não solicitadas.

- Mensagens com assuntos confidenciais não devem ser impressas em impressoras compartilhadas sem a supervisão do remetente, para impedir que outro funcionário, que não tenha o devido acesso, tome conhecimento do conteúdo da impressão, ainda que inadvertidamente.

- O *e-mail* deve estar ativo sempre que o usuário estiver trabalhando no computador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal.

- É proibido aos administradores de rede ou *e-mail* ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.

- Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

4.2.2 Uso do Telefone

Seguem as regras que devem ser observadas por todos os colaboradores quando da utilização destas ferramentas:

- O uso de telefone localizado fora das dependências da BRIDGE para discussão de assuntos confidenciais pode ser necessário, porém pode gerar exposição de segurança, portanto, certifique-se de que não está sendo escutado por pessoas próximas.

- Não deixe mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas.

- Quando estiver coordenando uma teleconferência, certifique-se de que todos os participantes foram devidamente autorizados antes de começar a reunião.

4.2.3 Uso da Internet

Seguem as regras que devem ser observadas por todos os colaboradores quando da utilização desta ferramenta, inclusive da rede *wi-fi* corporativa em dispositivos pessoais:

- Alguns *sites* (páginas da internet) contêm ou distribuem material não apropriado ao ambiente de trabalho, portanto, os colaboradores não devem acessar tais *sites* nem tampouco distribuir/obter material similar enquanto nas premissas da BRIDGE.

- Os acessos a *sites* podem estar sendo monitorados a qualquer tempo, portanto, em caso de dúvida, verifique junto a seu gestor ou à área de Tecnologia se o respectivo *site* pode ser acessado pelos colaboradores; alguns *sites*, inclusive, já foram bloqueados para o acesso dos colaboradores (ex: *web mails pessoais*, mídias sociais, páginas com conteúdo pornográfico).

- Não é permitido o uso de serviços de mensagens ou *chat* para uso pessoal (ICQ, AIM, Messenger, etc), com exceção do *Skype for Business* para uso restritamente profissional e somente com outros colaboradores da BRIDGE.

- Os serviços de mensagens fornecidos pela BRIDGE apenas devem ser utilizados para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas.

- Não é permitido o acesso das estações de trabalho a *Webmail* (Hotmail, Bol, Yahoo, UOL, AOL, etc.).

- Não é permitido o uso de compartilhadores de informações como redes *Peer-to-Peer*, também conhecidas como redes P2P (Kazaa, eDonkey, eMule, BitTorrent, etc.) dentro das dependências da BRIDGE.

- Não é permitido o *download* de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais.

4.2.4 Uso das impressoras

Seguem as regras que devem ser observadas por todos os colaboradores quando da utilização deste equipamento:

- Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora.

- Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários.

- A impressora apenas deve ser utilizada para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela BRIDGE.

- Impressões coloridas apenas devem ser feitas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

4.3 Senhas

A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do colaborador, portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

- Manter sua confidencialidade.

- Criar senhas fortes, respeitando, ao menos, os critérios abaixo:

  - ✓ As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex: nome ou data de nascimento do usuário).

  - ✓ Devem ter pelo menos 6 caracteres;

  - ✓ Devem conter pelo menos dois caracteres alfabéticos.

  - ✓ Devem conter pelo menos dois caracteres numéricos.

  - ✓ Devem conter pelo menos um caractere especial (! @ # $ % & *).

- Trocar a senha pelo menos a cada 3 meses.

- Evitar escrever a senha e, caso seja necessário, guardar a senha em local seguro.

Para facilitar, seguem exemplos de senhas fortes, fáceis de lembrar:

- eSu$6C (eu SEMPRE uso seis 6 CARACTERES, o “$” substitui o “s”).

- 9$Sgianc (9 senhas SEGURAS garantem integridade a nossa corporação).

- s&Nh45 (palavra senhas onde o & substitui o “e”, “4” o “a” e “5” o “s”).

- 3GdMpB! (eu GOSTO de MPB! , onde o 3 substitui o “E”).

Ressalte-se que essas senhas do exemplo não são mais seguras. Não as utilize.

4.4 Proteção do patrimônio

Integram o patrimônio físico e intelectual da BRIDGE seus móveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos funcionários, não podendo os mesmos ser utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos da BRIDGE para fins particulares, salvo se previamente autorizado pelo superior hierárquico imediato, sendo a referida aprovação vetada nos casos em que esta:

- Interferir no seu trabalho.
- Interferir ou concorrer com os negócios da BRIDGE.
- Fornecer informação a terceiros.
- Envolver solicitação comercial ou outra solicitação não apropriada ao negócio.
- Envolver custo adicional para a BRIDGE.

4.5 Proteção contra vírus e ataques

O vírus de computador é um programa desenhado para causar perda ou alteração de dados, com isso em vista, todo equipamento computacional da BRIDGE deve ter um programa antivírus instalado.

Os *softwares* de antivírus devem ser atualizados diariamente e de forma automática.

O colaborador, ao receber algum *e-mail* alertando sobre vírus, não deve encaminhá-lo a outras pessoas, pois geralmente estes alertas são falsos. De toda forma, permanecendo a dúvida, o colaborador deve entrar em contato com a área de Tecnologia para maiores explicações e suporte técnico.

4.6 Vulnerabilidades

O Sistema Operacional deve sempre estar atualizado, para isso, ele deve estar configurado para atualização automática.

4.7 Aquisição de *software* e direitos autorais

A maioria das informações e *softwares* que estão disponíveis em domínio público (incluindo a internet) está protegida por leis de Propriedade Intelectual, portanto:

- Não é permitido obter *softwares*, imagens, etc (*download*) destas fontes para uso na BRIDGE, exceto quando houver permissão explícita por parte do respectivo proprietário e autorização interna.
- Deve-se ler e compreender todas as restrições dos direitos autorais do *software* e, caso a BRIDGE não possa cumprir com as condições estipuladas, não é permitido fazer *download* e/ou utilizar o respectivo material.
- O colaborador deve garantir que cumpre com os requerimentos ou limitações do *software* (por exemplo, não pode ser utilizado para fins comerciais, não cobrar de outros o uso do *software*, etc.) antes de realizar o respectivo *download*.
- É proibido o uso de qualquer foto, imagem ou desenho que possua marca registrada de terceiros. Podem ser utilizadas imagens originais do Sistema Operacional ou imagens não relacionadas a Produtos, Empresas ou Pessoas. Imagens consideradas agressivas também não devem ser utilizadas.

- Em caso de dúvidas em relação às licenças ou a qualquer dos pontos acima, o colaborador deve entrar em contato com o *Compliance*.

4.8 *Backup* e restauração de sistemas

A importância dos *backup*s na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um incidente de segurança.

Cada departamento/usuário tem acesso a pelo menos uma pasta no servidor de arquivos. Todos os documentos relacionados ao negócio devem ser copiados nestas pastas.

Além disso, cada usuário tem uma pasta pessoal no servidor de arquivos. O *backup* de dados pessoais nas estações de trabalho é de total responsabilidade do usuário.

O *backup* dos servidores é executado pela equipe de Tecnologia responsável pelo mesmo.

Os *backup*s são realizados todos os dias com retenção em disco por 1 (uma) semana. No primeiro dia de cada mês, duas cópias completas de todos os arquivos são realizadas e armazenadas, a primeira em uma área reservada dentro das dependências da BRIDGE e a segunda em mídia localizada fora das referidas dependências.

4.9 Mesa limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens da BRIDGE, incluindo, mas não se limitando a papéis, *pen-drives*, CDs ou quaisquer outros tipos de mídias removíveis, acessíveis a outras pessoas sem a devida proteção, quando o funcionário estiver fora de sua estação de trabalho.

Caso a estação de trabalho do colaborador esteja situada em sala com porta e a respectiva porta possua tranca, o colaborador também pode trancar sua sala ao sair para evitar a exposição de informações confidenciais.

Ao final do dia de trabalho, computadores portáteis devem ser trancados em gaveta ou armário ou levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.

4.10 Tela limpa

Computadores, *notebooks* e *handhelds* devem estar protegidos por senha quando não estiverem sendo assistidos.

Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento por inativação.

4.11 Notificações de incidentes de segurança

Qualquer suspeita de ocorrência de incidente de segurança deve ser informada à equipe de Tecnologia. Nenhum colaborador deve investigar por conta própria ou tomar ações para se defender de eventual ataque, a não ser que seja instruído desta forma pela área de Tecnologia. A área de Tecnologia está capacitada para conter as exposições, analisar os impactos à BRIDGE e conduzir investigações, coletando evidências para possíveis ações jurídicas.

5. POLÍTICA DE SIGILO DA INFORMAÇÃO

Esta Política tem os seguintes objetivos:

a) Expor as normas e procedimentos de proteção do sigilo das informações, em cumprimento das determinações legais aplicáveis, em especial às normas que tratam do sigilo bancário.

b) Evitar a divulgação de dados e informações sobre as operações passivas (relacionamento com clientes) e ativas (operações com ativos sob gestão/administração) da BRIDGE, de forma a mantê-las sob sigilo.

c) Determinar as condições em que dados e informações sobre as operações passivas (relacionamento com clientes) e ativas (operações com ativos sob gestão/administração) da BRIDGE podem ser reveladas a terceiros.

A aplicação e monitoramento da Política de Sigilo das Informações cabe ao Departamento de *Compliance*, obedecidas as especificações adiante elencadas:

a) Os colaboradores devem proteger a confidencialidade de quaisquer informações obtidas durante o exercício de suas funções na BRIDGE, que não devem ser divulgadas a terceiros e/ou divulgadas ou disponibilizadas em domínio público.

b) A obrigação de sigilo prevista acima se aplica mesmo após a rescisão do vínculo do colaborador com a BRIDGE, qualquer que seja a razão, permanecendo o colaborador obrigado a manter sigilo e a proteger a confidencialidade das informações obtidas durante o exercício de suas funções na BRIDGE.

c) Todo documento ou informação criado ou que transita na BRIDGE deve ser classificado como público ou confidencial. São considerados documentos/informações confidenciais ("Informações Confidenciais"), aqueles que não devem ser colocados em domínio público ou disponibilizados/divulgados a terceiros, a saber:

- operações, estratégias, resultados, ativos, dados e projeções relativos às operações ativas e passivas da BRIDGE, em especial aqueles que possam levar a uma vantagem competitiva da BRIDGE frente a seus concorrentes;
- informações ou documentos que contenham informações sobre os planos de negócios da BRIDGE.
- informações confidenciais ou documentos que contenham informações confidenciais sobre colaboradores da BRIDGE.
- informações ou documentos que contenham informações sobre clientes, distribuidores e fornecedores da BRIDGE.
- informações ou documentos que contenham informações relativas às atividades da BRIDGE ou às suas controladas e controladoras, incluindo, mas não se limitando a textos, projetos, análises, informações relativas a clientes, colaboradores, prestadores de serviço, parceiros comerciais, dados de cotistas e operações financeiras, inclusive dados pessoais dos envolvidos, informações de emissores de títulos e valores mobiliários, estruturas de operações de financiamentos, incluindo seus envolvidos, segredos de mercado, *know-how*, melhorias, programas de treinamento, manuais ou materiais, informações técnicas, fontes codificadas de linguagem de

computador, contratos, procedimentos, listas de mala direta, listas de preços, dados financeiros ou de outra natureza, planos de negócios, livros de códigos, faturas ou quaisquer outros relatórios financeiros, programas de computador, sistemas de *software*, base de dados, discos e impressos, planos (comerciais, técnicos ou quaisquer outros), correspondências, relatórios internos, arquivos pessoais, material de vendas e propaganda, estratégia de *marketing*, números de telefone, nomes, endereços, estudos, compilações, previsões, informações técnicas, financeiras ou comerciais, informações pessoais de terceiros ou quaisquer outras informações, escritas ou não.

d) Questões envolvendo Informações Confidenciais de titularidade da BRIDGE não devem ser discutidas pelos colaboradores em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes, etc.

e) Os programas de correio eletrônico (*e-mails*) disponibilizados pela BRIDGE devem ser utilizados exclusivamente para mensagens de âmbito profissional e não podem, em hipótese alguma, ser usados para transmitir ou retransmitir mensagens ou seus anexos de qualquer natureza e conteúdo que possam comprometer a BRIDGE.

f) Os colaboradores que exercem atividade de gestão de recursos, no âmbito da equipe de gestão da BRIDGE, devem se abster do uso dos aparelhos celulares (telefonia ou dados) durante o horário de funcionamento de mercado, de modo a evitar o recebimento de informações de terceiros ou a transmissão de informações a terceiros, que possam ser qualificadas como *insider trading* ou como *front running*.

g) A BRIDGE veda o acesso interno dos colaboradores a redes sociais e sítios de relacionamento, sítios pornográficos e similares. Os colaboradores não devem se utilizar de seus aparelhos telefônicos, no ambiente de trabalho, para acessar os endereços bloqueados, sem prévia e expressa aprovação de sua chefia direta e desde que haja necessidade de uso com finalidade profissional.

h) Os colaboradores respondem individualmente, civil e criminalmente, pela divulgação indevida de Informações Confidenciais ou pela divulgação de quaisquer informações que tenham por objetivo atingir a honra ou a imagem da BRIDGE ou dissuadir seu relacionamento com clientes.

i) A BRIDGE adota a política de mesas limpas. Todos os colaboradores devem evitar manter papéis e documentos confidenciais expostos em suas mesas de trabalho. Documentos confidenciais devem ser guardados em local apropriado e com chave, mesmo no decorrer do expediente, para evitar o acesso de terceiros não autorizados. Ao final do expediente, os gaveteiros devem permanecer trancados e as mesas sem papéis ou documentos.

j) As Informações Confidenciais de clientes enviadas ou entregues à BRIDGE para execução de transações são protegidas por lei. O compartilhamento destas Informações Confidenciais com terceiros depende de expressa autorização dos clientes, por escrito, e precisa ser aprovado previamente pelo Compliance.

k) Nas operações passivas da BRIDGE, em especial quando se tratar de distribuição de cotas de fundos a clientes, os colaboradores devem firmar documentos específicos com os distribuidores dos fundos sob administração ou gestão, com dispositivos prevendo:

- a obrigação de os distribuidores adotarem política de privacidade e confidencialidade de dados dos clientes.

- a garantia aos clientes da devida observância destas políticas pelo distribuidor e pelas pessoas a ele vinculadas.

- minimizar riscos de imagem para a BRIDGE, evitando que clientes vinculem a BRIDGE a uma eventual falha do distribuidor na proteção das Informações Confidenciais.

l) Os dados e as operações dos fundos sob administração ou gestão e dos respectivos cotistas podem ser informados por ordem ou pedido escrito do Banco Central do Brasil, da Comissão Valores Mobiliários e de autoridades judiciais, dentro dos casos previstos na legislação em vigor.

6. PLANO DE CONTINUIDADE DOS NEGÓCIOS

A BRIDGE formulou o presente Plano de Continuidade dos Negócios ("Plano") com o objetivo de nortear a forma de identificar, prevenir e atuar em situações de contingência, definindo as áreas prioritárias e procedimentos para garantir a continuidade das atividades realizadas cotidianamente.

A área de *Compliance* deve se certificar da implementação do Plano para garantir a continuidade dos processos críticos da instituição em casos de eventos inesperados que afetem parte ou a totalidade da capacidade operacional da BRIDGE, assegurando a realização de testes periódicos que atestem sua efetividade.

Dentre os principais eventos a serem considerados, podem ser verificados os seguintes:

- incêndio;
- alagamento;
- sabotagem;
- terrorismo/pirataria;
- furacão;
- desordem civil;
- roubo;
- falta de energia;
- falha aleatória de sistema crítico para a BRIDGE.

6.1. Modelo de atividade, infraestrutura e necessidades do negócio

A BRIDGE é uma instituição não-financeira focada na atividade de administração fiduciária de fundos para gestores independentes e clientes institucionais, bem como na atividade de gestão de recursos para fundos.

6.1.1 Infraestrutura física e tecnológica

As necessidades da BRIDGE no que tange aos recursos físicos e tecnológicos tendem a crescer com o desenvolvimento do negócio, no entanto, considerando que atualmente os serviços de controladoria prestados aos fundos de investimento sob administração fiduciária, exceto em relação a alguns FIPs, bem como os serviços de custódia dos fundos sob administração da BRIDGE são terceirizados com outras instituições autorizadas pela CVM, a continuidade das atividades da BRIDGE em caso de desastres, interrupção parcial de acesso às instalações físicas ou restrição de acesso aos recursos tecnológicos deve ser garantida conforme abaixo:

- Energia: o acesso à energia é básico para o funcionamento do escritório da BRIDGE. Assim, as nossas instalações contam com sistema *No-Break* de 40 KVA, muito acima da necessidade da empresa. O sistema foi dimensionado para garantir a energia para 90 pessoas por 18 minutos. Numa simples regra de três, em caso de falta de luz, podemos reduzir o atual número de funcionários para número especialmente restrito que funciona em contingência. Caso este número seja de 3 funcionários, há energia suficiente para 9 horas ininterruptas.

- Internet: o acesso é primordial para as consultas de portfólio e cadastros de movimentações no *website* do controlador terceirizado. A contingência primária é dada pela redundância natural, uma vez que o serviço contratado pela BRIDGE já é atualmente fornecido por 2 (dois) provedores finais.

- Restrição de acesso físico: em caso de indisponibilidade de acesso às instalações físicas, o plano de trabalho deve ser feito via acesso à Internet existente nas residências de seus sócios e funcionários, bem como acesso remoto à rede interna autorizado especificamente aos colaboradores cujas funções são essenciais à continuidade do negócio.

- Acesso remoto (Acesso *VPN* via *Network Connect*): deve ser provido acesso remoto à rede interna da BRIDGE para alguns colaboradores considerados críticos, para que, em caso de contingência, estes tenham a possibilidade de acessar arquivos nela localizados e, assim, possam dar continuidade às atividades que realizam cotidianamente. Para definir quais são estes colaboradores críticos, deve se levar em consideração: (i) as atividades realizadas; (ii) a criticidade de tais atividades; (iii) a periodicidade de realização de tais atividades; (iv) a necessidade de utilização de arquivos localizados na rede interna para a execução completa de tais atividades.

  A equipe de Tecnologia deve viabilizar o referido acesso: (i) fornecendo credencial de acesso remoto para os colaboradores críticos; (ii) auxiliando tais colaboradores a instalarem o Java em suas máquinas pessoais; e (iii) esclarecendo quaisquer dúvidas dos colaboradores durante a instalação e a utilização deste acesso.

- *E-mail*: o acesso ao correio eletrônico corporativo de domínio bridgetrust.com também é uma ferramenta primordial para receber instruções dos gestores independentes. Pensando nisso, a BRIDGE usa a tecnologia disponível do Microsoft Office 365, com correio eletrônico em “nuvem” redundante da Microsoft. Vale ressaltar que

outras formas de contingência, como a passagem de ordens por telefone (com *call back*), também funcionam.

- Telefonia: é possível receber chamadas via ramal com tecnologia IP de forma remota e a telefonia celular própria dos funcionários também pode ser utilizada para solução básica de contingência. Vale ressaltar que informações, tais como os contatos das contrapartes, já possuem redundância do MS Outlook 365 na "nuvem" Microsoft.

- Acesso aos arquivos: o modelo de redundância é via guarda de arquivos em discos rígidos removíveis com padrão de conexão USB, de forma que tais discos possam ser facilmente acessados via os computadores pessoais de sócios e funcionários da BRIDGE. Para garantir o acesso físico aos dados, as cópias de segurança são gravadas em dois discos rígidos removíveis, que se alternam a cada semana, sendo que o outro fica guardado fora das instalações da BRIDGE.

- *Backups*: os *backups* são realizados todos os dias com retenção em disco por 1 (uma) semana. No primeiro dia de cada mês, duas cópias completas de todos os arquivos são realizadas e armazenadas, a primeira em uma área reservada dentro das dependências da BRIDGE e a segunda em mídia localizada fora das referidas dependências.

- Restauração dos sistemas: a área Administrativa, junto ao departamento de Tecnologia, é responsável por manter disponível toda a documentação necessária, bem como todos os dados e *softwares* necessários para a restauração dos sistemas.

6.1.2. Serviços terceirizados (diligência na contratação de prestadores de serviço)

A BRIDGE, na condição de instituição administradora, pode deliberadamente, a seu exclusivo critério, terceirizar outros serviços desde que garanta, também com base em sua "Política de Seleção, Contratação e Supervisão de Prestadores de Serviços para Fundos de Investimento sob Administração e Gestão", que os prestadores contratados (i) apresentem toda documentação necessária em conformidade com os padrões da BRIDGE; (ii) possuam procedimentos e controles adequados ao ambiente regulatório e práticas de mercado; (iii) possuam reputação e imagem íntegras e idôneas; e (iv) possuam infraestrutura adequada à prestação dos serviços objeto de sua contratação, a fim de assegurar, entre outros, que os respectivos serviços não sejam interrompidos em caso de eventuais indisponibilidades.

6.1.3. Ausência temporária dos diretores estatutários

Conforme disposto em contrato social, no caso de ausência temporária ou impedimento eventual de qualquer um dos Diretores da BRIDGE, nomeados no referido contrato, em relação às suas funções administrativas, as decisões de sua competência serão tomadas interinamente pelo Diretor Presidente, também nomeado no referido contrato. Na ausência temporária ou impedimento eventual do Diretor Presidente, as decisões de sua competência serão tomadas em reunião de Diretoria com a presença mandatória de todos os Diretores Executivos. Em caso de vacância permanente de qualquer um dos Diretores, deverá ser imediatamente convocada uma reunião de sócios para deliberar a eleição de seu substituto.

6.2. Plano de ação

Em algumas situações de contingência, será necessário adotar as medidas abaixo:

6.2.1 Impossibilidade de acessar a sede da BRIDGE

- Ligar para o gestor de sua área e verificar como proceder;
- Se tiver subordinados, ligar para eles e indicar-lhes como proceder;
- Acessar o grupo da BRIDGE no *whatsapp* para maiores informações;
- Caso seja solicitado pelo gestor de sua área, direcionar-se ao ponto de encontro localizado na Praia de Botafogo, nº 400, no bairro de Botafogo, Rio de Janeiro/RJ, em frente ao Botafogo Praia Shopping.

6.2.2. Necessidade de trabalhar remotamente

- Todos os funcionários possuem acesso ao *webmail* via internet;
- A grande maioria dos sistemas da BRIDGE ficam localizados em nuvem, portanto, todos os colaboradores que possuem acesso a estes sistemas poderão conectar-se via internet;
- Os colaboradores críticos devem acessar à rede interna via acesso remoto - VPN, previamente instalado em seus computadores pessoais. Os computadores localizados nas estações de trabalho destes funcionários deverão ser mantidos permanentemente ligados para que seja possível a conexão remota quando necessária. Todas as regras estabelecidas nesse Manual são integralmente aplicáveis aos colaboradores que utilizam o acesso remoto.

6.2.3. Necessidade de evacuação

- O edifício onde está localizada a BRIDGE possui plano de evacuação, portanto, este deverá ser respeitado.
- Após evacuar o edifício, o colaborador deverá seguir para o ponto de encontro estabelecido pelo edifício, localizado do outro lado da rua em frente à entrada principal do Centro Empresarial Mourisco, e, caso necessário, para o ponto de encontro estabelecido pela BRIDGE, localizado na Praia de Botafogo, nº 400, no bairro de Botafogo, Rio de Janeiro/RJ, em frente ao Botafogo Praia Shopping.

6.3. Testes e apuração da qualidade da estrutura de contingência

A área de *Compliance* é responsável, com o auxílio da área Administrativa e de Tecnologia, por organizar, coordenar e supervisionar testes de contingência periódicos. Nesses testes, todos os procedimentos devem ser executados em sua integridade, a fim de identificar os pontos falhos na contingência e aprimorá-los.

Periodicamente, são realizados testes efetivos da estrutura de *backup* e de acesso remoto, bem como realizados quaisquer ajustes que se tornem necessários.

Cabe às áreas envolvidas garantir que quaisquer mudanças/ajustes necessários sejam realizados em tempo hábil.

Além disso, periodicamente o Centro Empresarial Mourisco, edifício onde está localizado a sede da BRIDGE, realiza simulações de evacuação para testar os procedimentos relacionados. Todos os colaboradores da BRIDGE presentes nos dias dos referidos testes deverão participar deles.

7. CONSIDERAÇÕES FINAIS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios, portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar a área de *Compliance*.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, medidas administrativas ou judiciais cabíveis, podendo levar à demissão ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

Este documento está disponibilizado ao público em geral na página da BRIDGE na rede mundial de computadores, nos termos da Instrução CVM 558.

A expectativa da alta administração da BRIDGE é que em até 6 (seis) meses a contar da última revisão deste documento, todos os controles e estruturas aqui citados já estejam em vigor em caráter efetivo, sendo certo que alguns deles já estão em pleno funcionamento nesta data.