MANUAL DE REGRAS, PROCEDIMENTOS E CONTROLES INTERNOS

ATUALIZAÇÃO: 14/02/2019

SUMÁRIO

1. POLÍTICA DE COMPLIANCE

Este Manual de Regras, Procedimentos e Controles Internos da Warren Brasil Gestão e Administração de Recursos Ltda. ("Warren" e "Manual de Compliance", respectivamente) visa estabelecer meios de controles internos adequados ao nível de complexidade e risco das operações realizadas pela Warren, além do permanente atendimento às normas, políticas, regulamentações vigentes e políticas internas da Warren.

Este Manual de Compliance é aplicável a todos os sócios, administradores, empregados, funcionários, trainees e estagiários da Warren (em conjunto os "Colaboradores" e, individualmente e indistintamente, o "Colaborador").

1.1 Introdução

O termo compliance é originário do verbo, em inglês, to comply, e significa "estar em conformidade com regras, normas e procedimentos".

Visto isso, a Warren adota em sua estrutura controles internos adequados à estrutura da Warren, para o permanente atendimento às normas, políticas e regulamentações vigentes e outras políticas internas da Warren (controles internos), que devem efetivamente ser cumpridas, seguidas e respeitadas.

Por meio dos controles de compliance, qualquer desvio em relação aos controles internos da Warren é observado e minimizado.

O Manual de Compliance foi desenvolvido com vistas a dar cumprimento às obrigações estabelecidas na Instrução CVM nº 558/15, nos Códigos de autorregulação da ANBIMA dos quais a Warren seja aderente, bem como demais normas, diretrizes e Ofícios de Orientação emitidos pelos referidos órgãos de regulação e autorregulação, dentre outras melhores práticas nacionais e internacionais aplicáveis às atividades da Warren.

1.2 Função do Departamento de *Compliance*

1.2.1 Responsabilidades

São responsabilidades do departamento de *compliance* da Warren:

i. Assegurar que toda a equipe esteja operando de acordo com as diretrizes e políticas estabelecidas pela Warren;

ii. Descrever, avaliar e revisar os procedimentos das áreas visando minimizar falhas operacionais;

iii. Estabelecimento de normas, procedimentos e controles internos; e

iv. A revisão e atualização periódica das Políticas Internas e do Manual de Compliance.

1.2.2 Atividades Principais

i. Emissão de regulamentos e normas internas;

ii. Testes de *compliance* em operações, procedimentos e cadastros;

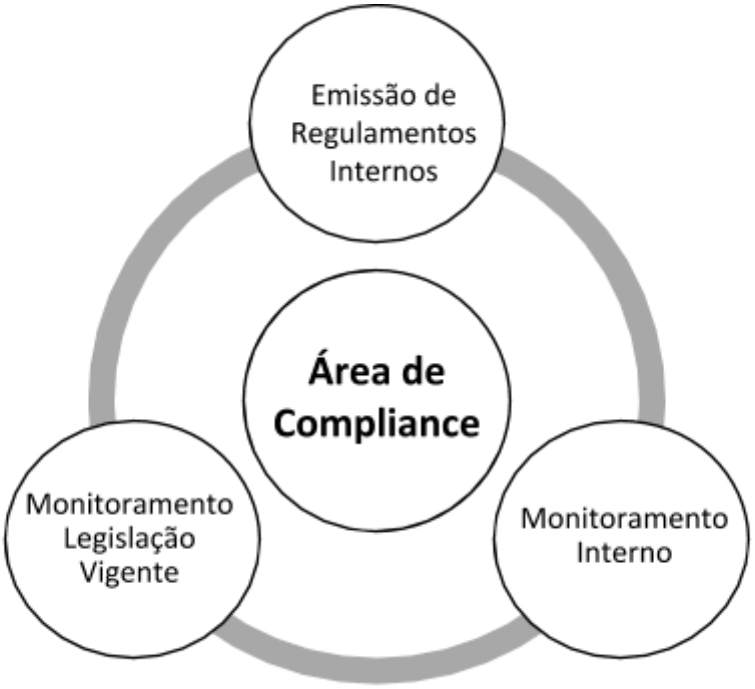
iii. Monitoramento e implementação de mecanismos de controles internos;

iv. Criação e manutenção de plano de continuidade dos negócios;

v. Pesquisa de legislação aplicável às atividades da Warren no que se refere a compliance e controles internos; e

vi. Controle e revisão de erros ou falhas que gerem perdas financeiras efetivas ou potenciais.

A Área de Compliance da Warren possui como base de sua atuação três pontos: i) Emissão de regulamentos e normas; ii) Fiscalização e monitoramento interno e iii) Conformidade com a legislação vigente.



O monitoramento interno tem como foco garantir a segurança da informação e garantir que os colaboradores sigam as normas e procedimentos de segurança estabelecidos. Para isso, são realizados monitoramentos e relatórios que asseguram cada item.

1.3 Função do Responsável pelo Compliance (Gerente de Compliance)

O *Gerente de Compliance* tem como principais atribuições e responsabilidades o suporte a todas as áreas da Warren no que concerne a esclarecimentos de todos os controles e regulamentos internos (*compliance*), bem como no acompanhamento de conformidade das operações e atividades da Warren com as normas regulamentares (internas e externas) em vigor, definindo os planos de ação, monitorando o cumprimento de prazos e do nível de excelência dos trabalhos efetuados e assegurando que quaisquer desvios identificados possam ser prontamente corrigidos (*enforcement*).

O *Gerente de Compliance* não atua em outras áreas que possam comprometer sua independência na função de responsável pelo *Compliance* e possuirá suas atividades supervisionadas pelo Diretor de Compliance.

Ressaltamos que o *Gerente de Compliance* é, também, o responsável pela observância dos parâmetros e procedimentos relativos à precaução à lavagem de dinheiro, conforme disposto na "Política de *Know Your Client* e Prevenção à Lavagem de Dinheiro" da Warren.

Ainda, são também atribuições do *Gerente de Compliance*, sem prejuízo de outras descritas neste Manual de *Compliance*:

i. Estabelecer os princípios éticos que deverão ser seguidos por todos os superiores e Colaboradores, conforme devidamente destacado no "Código de Ética" da Warren ou de quaisquer documentos que possam ser produzidos para essa finalidade, elaborando sua revisão periódica;

ii. Implantar o conceito de controles internos através de uma cultura de *compliance*, visando melhoria nos controles;

iii. Definir a política e controle sobre investimentos pessoais dos Colaboradores, em acordo com as diretrizes estabelecidas na *'Política de Compra e Venda de Valores Mobiliarios'*;

iv. Propiciar o amplo conhecimento e execução dos valores éticos na aplicação das ações de todos os Colaboradores;

v. Analisar todas as situações acerca do não-cumprimento dos procedimentos ou valores éticos estabelecidos neste Manual de *Compliance*, ou no "Código de Ética", assim como avaliar as demais situações que não foram previstas nas políticas internas da Warren;

vi. Definir estratégias e políticas pelo desenvolvimento de processos que identifiquem, mensurem, monitorem e controlem contingências;

vii. Assegurar o sigilo de possíveis delatores de crimes ou infrações, mesmo quando estes não pedirem, salvo nas situações de testemunho judicial;

viii. Solicitar a tomada das devidas providências nos casos de caracterização de conflitos de interesse;

ix. Reconhecer situações novas no cotidiano da administração interna ou nos negócios da Warren que não foram planejadas, fazendo a análise de tais situações;

x. Propor estudos para eventuais mudanças estruturais que permitam a implementação ou garantia de cumprimento do conceito de segregação das atividades desempenhadas pela Warren;

xi. Verificar, no mínimo anualmente, se os "colaboradores-chave", em especial os sócios controladores e os Diretores de áreas reguladas, estão envolvidos em processos administrativos de órgãos reguladores e autorreguladores, criminais de qualquer natureza, ou ainda outros processos que possam trazer contingências para a Warren e que, portanto, torne sua divulgação pública necessária, nos termos da Instrução CVM 558/15;

xii. Confirmar, por meio do CVMWEB, entre os dias 1º e 31 de maio de cada ano, que as informações contidas no formulário cadastral da Warren previsto na Instrução CVM 510/11 continuam válidas, bem como atualizar o referido formulário cadastral sempre que qualquer dos dados neles contido for alterado;

xiii. Para cumprimento da ICVM 558, o *Gerente de Compliance* deverá enviar o Formulário de Referência, por meio de sistema eletrônico da CVM, até o dia 31 de março de cada ano.

xiv. Providenciar atendimento a fiscalizações e supervisões de órgãos reguladores e autorreguladores, auditorias terceirizadas e due dilligences, fazendo a interface entre as solicitações destes e as áreas internas da Warren; e

xv. Examinar de forma sigilosa todos os assuntos que surgirem, preservando a imagem da Warren, assim como das pessoas envolvidas no caso.

Na execução das atividades sob sua responsabilidade, estabelecidas neste Manual de Compliance ou fora dela, poderá se utilizar de sistemas eletrônicos e/ou serviços de advogados ou firmas de consultoria de Compliance para suporte e auxílio em suas funções.

1.4 Relatório anual de acompanhamento

Para assegurar a eficácia deste Manual de *Compliance*, o *Gerente de Compliance* deverá encaminhar aos sócios e diretores da Warren, inclusive os diretores responsáveis pela administração de carteiras da Warren, até o último dia útil do mês de janeiro de cada ano, relatório relativo ao ano civil imediatamente anterior à data de entrega, contendo: (i) as conclusões dos exames efetuado; (ii) recomendações a respeito de eventuais deficiências, com o estabelecimento de cronogramas de saneamento, quando for o caso; e (iii) manifestação do diretor responsável pela gestão dos Fundos, ou, quando for o caso, pelo diretor responsável pela gestão de risco a respeito das deficiências encontradas em verificações anteriores e das medidas planejadas, de acordo com cronograma específico, ou efetivamente adotadas para saná-las ("Relatório Anual de *Compliance*"), conforme modelo previsto no Anexo I.

1.5 Revisão e Avaliação

O presente Manual de *Compliance* deverá ser revisto e atualizado ao menos anualmente.

2. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Nos termos da Instrução CVM nº 558, de 26 de março de 2015, especialmente o Artigo 24, III e Artigo 25, II, a Warren adota procedimentos e regras de condutas para preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas.

Todos os colaboradores, sócios e prestadores de serviços da Warren recebem treinamento referente ao Código de Ética e Política de Segurança da Informação (conforme descrito no item 6 desse manual). Além disso, assinam o Termo de Compromisso, que se encontra no Anexo II (está disponível também nos anexos do Código de Ética). A partir desse termo, o colaborador, sócio ou prestador de serviço declara estar ciente das proibições e restrições descritas no presente Manual e manter o sigilo e comportamento ético frente a informações confidenciais.

2.1 Política de Confidencialidade, segregação de atividades e Segurança da Informação

A informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Warren é considerada confidencial e não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

2.1.1 Segurança da informação confidencial

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da Warren, que não necessitem de, ou não devam ter acesso a, tais informações para desempenho de suas atividades profissionais.

Qualquer informação sobre a Warren, ou de qualquer natureza relativa às atividades da Warren, aos seus sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Warren, só poderá ser fornecida ao público, mídia ou a demais órgãos caso autorizado por escrito pelo *Gerente de Compliance*.

É terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Warren e circulem em ambientes externos à Warren com estes arquivos, uma vez que tais arquivos contêm informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Warren e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Warren.

O descarte de informações confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação. Todos os arquivos digitalizados em pastas temporárias serão apagados periodicamente, de modo que nenhum arquivo deverá ali permanecer. A desobediência a esta regra será considerada uma infração, sendo tratada de maneira análoga à daquele que esquece material na área de impressão.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

Adicionalmente, os Colaboradores devem se abster de utilizar *hard drives*, *pen-drives*, *disquetes*, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Warren.

É proibida a conexão de equipamentos na rede da Warren que não estejam previamente autorizados pela área de informática e pela área de *compliance*.

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

O envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Warren.

Em nenhuma hipótese um Colaborador pode emitir opinião por e-mail em nome da Warren, ou utilizar material, marca e logotipos da Warren para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

A Warren se reserva no direito de gravar qualquer ligação telefônica e/ou qualquer comunicação dos seus Colaboradores realizada ou recebida por meio das linhas telefônicas ou qualquer outro meio disponibilizado pela Warren para a atividade profissional de cada Colaborador.

2.1.2 Informação Privilegiada

É considerada como informação privilegiada qualquer Informação Relevante (conforme definido abaixo) a respeito de alguma empresa, que não tenha sido publicada e que seja conseguida de maneira privilegiada, em consequência da ligação profissional ou pessoal mantida com um cliente, com colaboradores de empresas estudadas ou investidas ou com terceiros, ou em razão da condição de Colaborador.

Considera-se Informação Relevante, para os efeitos deste Manual de *Compliance*, qualquer informação, decisão, deliberação, ou qualquer outro ato ou fato de caráter político-administrativo, técnico, negocial ou econômico-financeiro ocorrido ou relacionado aos negócios da Warren que possa influir de modo ponderável: (a) na rentabilidade dos valores mobiliários administrados pela Warren; (b) na decisão de investidores de comprar, vender ou manter cotas de fundos de investimento administrados pela Warren; e (c) na decisão dos investidores de exercer quaisquer

direitos inerentes à condição de titular de cotas de fundos de investimento administrados pela Warren.

As informações privilegiadas precisam ser mantidas em sigilo por todos que a acessarem, seja em função da prática da atividade profissional ou do relacionamento pessoal.

Em caso do Colaborador ter acesso a uma informação privilegiada que não deveria ter, deverá transmiti-la rapidamente ao *Gerente de Compliance*, não podendo comunicá-la a ninguém, nem mesmo a outros membros da Warren, profissionais de mercado, amigos e parentes, e nem usá-la, seja em seu próprio benefício ou de terceiros. Se não houver certeza quanto ao caráter privilegiado da informação, deve-se, igualmente, relatar o ocorrido ao *Gerente de Compliance*.

2.1.3 Insider trading e "dicas"

Insider trading baseia-se na compra e venda de títulos ou valores mobiliários com base no uso de informação privilegiada, com o objetivo de conseguir benefício próprio ou de terceiros (compreendendo a própria Warren e seus Colaboradores).

"Dica" é a transmissão, a qualquer terceiro, de informação privilegiada que possa ser usada com benefício na compra e venda de títulos ou valores mobiliários.

É proibida a prática dos atos mencionados anteriormente por qualquer membro da empresa, seja agindo em benefício próprio, da Warren ou de terceiros.

É de responsabilidade do Gerente de Compliance verificar e processar, trimestralmente, as notificações recebidas a respeito do uso pelos Colaboradores de informações privilegiadas, *insider trading* e "dicas". Casos envolvendo o uso de informação privilegiada, *insider trading* e "dicas" devem ser analisados não só durante a vigência do relacionamento profissional do Colaborador com a Warren, mas mesmo após o término do vínculo, com a comunicação do ocorrido às autoridades competentes, conforme o caso.

2.2 Política de Segregação de atividades – Separação física

Todas as áreas da Warren são segregadas, especialmente a área de gestão de recursos e administração fiduciária, que são segregadas entre si e das demais áreas da Warren, sendo o acesso restrito aos Colaboradores integrantes das respectivas áreas, por meio de controle de acesso nas portas.

Para garantir que não exista circulação de informações que possam gerar conflito de interesses ("*chinese wall*"), além do controle de acesso em todas as portas da Warren, todas as paredes contêm isolamento acústico.

Não será permitida a circulação de Colaboradores em seções que não destinadas ao respectivo Colaborador.

Reuniões com terceiros não Colaboradores serão agendadas em salas específicas destinadas a reuniões. Será feito o controle e triagem prévia do terceiro não Colaborador, sendo este encaminhado diretamente à sala de reunião.

É de competência do Gerente de Compliance, ao longo do dia, fiscalizar a presença dos Colaboradores em suas devidas seções, sendo, ainda, informado imediatamente por *e-mail* se o acesso às áreas restritas for negado aos Colaboradores por mais de 5 (cinco) vezes. O Gerente de Compliance elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções. Eventual infração à regra estabelecida será devidamente esclarecida e todos os responsáveis serão advertidos e passíveis de punições a serem definidas pelo Gerente de Compliance.

A propósito, as tarefas contábeis da empresa serão terceirizadas, de modo que sejam exercidas no local de atuação das empresas contratadas.

3. SEGURANÇA DA INFORMAÇÃO DIGITAL

A Warren é uma empresa com grande foco em tecnologia. Por isso, a segurança da informação e dos sistemas por onde essa informação transita é de grande importância. Para melhor compreensão, a segurança da informação é dividida em três níveis nesse manual:

- Acessos a sistemas – definição da política de logins, controles de acesso e monitoramento desses acessos pelos colaboradores da Warren;

- Segurança de infraestrutura – garantia de que os sistemas utilizados para as diversas atividades de Gestor de Recursos e Administrador Fiduciário são seguros em sua estrutura, possibilitando backups. Além disso, é importante a adequação da infraestrutura necessária para o trânsito das informações.

3.1 Acessos a sistemas

A área de Compliance é responsável por manter organizada a estrutura de acessos aos diretórios da Warren. Isso significa estabelecer uma hierarquia de acessos de acordo com cada área e cargo ocupado. A área de Compliance possui acesso a todas as áreas. Uma vez que são dados os acessos corretos, cabe ao Gerente de Compliance também monitorar e ser avisado por e-mail em caso de tentativa de acesso aos diretórios e *logins* virtuais no servidor protegidos por senha. O Gerente de Compliance elucidará as circunstâncias da ocorrência deste fato e aplicará as devidas sanções.

Programas instalados nos computadores, principalmente via internet (*downloads*), sejam de utilização profissional ou para fins pessoais, devem obter autorização prévia do responsável pela área de informática na Warren. Não é permitida a instalação de nenhum *software* ilegal ou que possua direitos autorais protegidos. A instalação de novos *softwares*, com a respectiva licença, deve também ser comunicada previamente ao responsável pela informática. Este deverá aprovar ou vetar a instalação e utilização dos softwares dos Colaboradores para aspectos profissionais e pessoais.

Em caso de divulgação indevida de qualquer informação confidencial, o Gerente de Compliance irá apurar o responsável por tal divulgação, sendo certo que poderá verificar no servidor quem teve acesso ao referido documento por meio do acesso individualizado de cada Colaborador (conforme previsto adiante).

3.1.1 Política de Segregação de atividades – dados eletrônicos

Cada Colaborador possuirá microcomputador e telefone de uso exclusivo, de modo a evitar o compartilhamento do mesmo equipamento e/ou a visualização de informações de outro Colaborador.

Os colaboradores com privilégios de acesso definidos pelo Gerente de Compliance podem acessar o ambiente da Intranet da Warren e fazer consultas pelos dados de clientes e fundos. O nível de privilégio de cada usuário é configurado no sistema pelo responsável de TI de acordo com a orientação do Gerente de Compliance.

A política de senhas de usuário internos seguem as seguintes normas:

- As senhas expiram após 60 dias;
- A senha não pode ser igual à uma das últimas 6 senhas.
- Ao menos 60% dos caracteres devem ser diferentes da senha anterior;
- A senha deve ter no mínimo 4 números, 3 letras e dois símbolos;
- Não estar presente na blacklist definida pelo Gerente de Compliance.

Ademais, não haverá compartilhamento de equipamentos entre os Colaboradores da área de administração de recursos e os demais Colaboradores, sendo que haverá impressora e *scanner* destinados exclusivamente à utilização da área de administração de recursos.

Especificamente no que diz respeito à área de informática e de guarda, conservação, restrição de uso e acesso a informações técnicas/arquivos, dentre outros, informamos que o acesso aos arquivos/informações técnicas será restrito e controlado,

sendo certo que tal restrição/segregação será feita em relação a: (i) cargo/nível hierárquico; e (ii) equipe.

Todos os acessos à Intranet da Warren são logados automaticamente, ficando o registro de acessos disponível ao Gerente de Compliance que irá realizar consultas aleatórias, regularmente, para fins de controle. Cada acesso gera um registro de uma chave única por máquina no banco de dados, permitindo o cruzamento dos acessos para controle de não compartilhamento de senhas. Da mesma forma, consultas recusadas por controle de acesso são registradas e listadas para acompanhamento de tentativas de acesso a informações sensíveis não autorizadas.

Ademais, cada Colaborador possuirá um código de usuário e senha para acesso à rede, o qual é definido pelo responsável de cada área, sendo que somente os Colaboradores autorizados poderão ter acesso às informações da área de administração de recursos. Ainda, a rede de computadores da Warren permitirá a criação de usuários com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores, garantindo que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por usuário. Além disso, a rede de computadores manterá um registro de acesso e visualização dos documentos, o que permitirá identificar as pessoas que têm e tiveram acesso a determinado documento.

Ainda, cada Colaborador terá à disposição uma pasta de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do usuário aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos na respectiva pasta serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

Os softwares de terceiros utilizados por cada colaborador deverão ser instalados e gerenciados pela área de Tecnologia da Informação. Eles também deverão ter acesso individualizado por meio de login e senha para cada usuário. Em caso de sistemas onde transitem informações consideradas confidenciais, conforme citadas no capítulo 2.1.2 desse manual, a empresa contratada deve garantir a segurança e integridade das informações, bem como possibilidade de *backup* pela Warren.

3.1.2 Testes periódicos de segurança

Trimestralmente, o Gerente de Compliance realiza testes de segurança da informação com o objetivo de validar cada um dos itens monitorados listados anteriormente. Os testes listados a seguir estão exemplificados no anexo III.

Item a ser verificado	Forma de Verificação
Verificação se o colaborador utilizou outra máquina para fazer login. Ou se houve login de outro colaborador na sua máquina.	Listagem de logins efetuados em cada computador.
Relatório de Impressões	Lista de logins que imprimiram em cada impressora.
Controle de Acesso e permissões a diretórios	Realizado pela área de Compliance.
Procedimentos de desligamento de funcionários.	Check-list com os itens a serem verificados: arquivos pessoais devem ser descartados e arquivos sobre a Warren devem ser mantidos.
Backup semanal	Número de arquivos salvos.

Em relação às informações, ainda são realizadas fiscalizações aleatórias trimestrais em relação ao acesso à internet, que contempla: possível compartilhamento de senhas e informações confidenciais e acesso ou tentativa de acesso a informações não autorizadas. As ligações telefônicas também são monitoradas de forma aleatória regularmente. O objetivo desse relatório é verificar a conformidade da atuação dos Colaboradores, tendo como objetivo a análise de 1% do total de acessos e telefonemas. Caso seja identificado alguma inconformidade, o Gerente de Compliance deverá autuar o Colaborador, que passará a ser monitorado mensalmente a fim de evitar as reincidências. O exemplo desse relatório está no Anexo IV.

3.2 Segurança de Infraestrutura

As infraestruturas de produção, homologação e desenvolvimento da Warren estão alocadas na infraestrutura da Amazon AWS. Os servidores foram contratados no regime de reserva de infraestrutura. Todo acesso para gerenciamento e controle dos ambientes é feito via autenticação utilizando o usuário do responsável pela TI.

O acesso remoto ao ambiente de produção é realizado apenas pelo responsável de TI através de autenticação utilizando chave privada criada com criptografia RSA. Os dados armazenados no banco de dados de produção são compactados de forma automática com agendamento diário e armazenados criptografados na nuvem como backup.

Os dados referentes à atividade da Warren circulam de duas formas: a primeira é de forma virtual, na nuvem. Todo tráfego de informação que passa pela nuvem está na Amazon (intranet e plataformas dos clientes) e no BRITech (software de gerenciamento do BackOffice). Por esse motivo, os testes de segurança estão focados em proteger esses dois ambientes.

A seguir, estão as características de controle de segurança da Britech e Amazon. No capítulo seguinte estão listados os testes de segurança dos ambientes na nuvem.

- **Britech –** software utilizado por grande parte das atividades de Administração Fiduciária (cotização dos fundos, por exemplo) no mercado. Esse sistema é terceirizado e apresenta como principais características de segurança:

    - Autenticação no login, registro das atividades realizadas, vedação de acesso simultâneo do mesmo login, política de senhas, possibilitando a customização das exigências de obrigatoriedades;

    - Nenhum dado trafegando como parâmetros de URL, conexão encriptada via SSL, Selo de Segurança do Site Bindado ©, execução de testes diários de segurança no site.

    - Os Sistemas da Plataforma ATLAS (Britech) oferecidos na modalidade SaaS estão hospedados em um ambiente seguro, que conta com firewall e ferramentas de monitoramento para evitar a interferência ou acesso de intruso.

    - Toda a Infraestrutura física é hospedada em data centers localizados em São Paulo. O data center segue as orientações do ITIL e tem sua qualidade assegurada por um sistema de gestão de certificado ISO 9001:2000, prezando continuamente pela segurança e qualidade de seus serviços. A mesma sofre avaliações periódicas para garantir a conformidade com os padrões de segurança da indústria.

    - Os data centers onde a nossa Solução SaaS fica hospedada possuem certificações (SSAE16, SAS70 tipo II, ISO) que atendem aos padrões internacionais incluindo SOX.

    - O acesso às bases de produção é restrito a um número limitado de pontos e as bases de produção não compartilham uma senha mestre.

    - Os funcionários da BRITech não têm acesso direto ao ambiente de produção, exceto quando necessário para manutenção do sistema, monitoramento e backups.

- Os backups de dados são realizados diariamente, de acordo com políticas previamente definida.

- **Amazon**: Possui certificado ISO 27001 e PCI, que atestam a segurança nos processos seguidos pela empresa, descritos anteriormente. A empresa disponibiliza ao público sua metodologia de testes e segurança através do site: https://aws.amazon.com/pt/compliance/.

3.2.1 Testes periódicos de segurança

Em relação aos sistemas utilizados, destacamos os testes de segurança a seguir.

BRITech

- São feitos mais de 32.000 testes divididos em 17 categorias no qual grande parte dessas categorias está alinhada com o TOP TEN da OWASP.

- É realizado, no mínimo uma vez por semana, testes considerados como críticos que são: 1) SQL Disclosure 2) Sql Error Message 3) Blind Sql Injection 4) Cross Site Scripting 5) Check http Method.

- Scan no Servidor (IP)

  - São feitos mais de 11.000 testes de vulnerabilidades + em centenas de aplicativos e sistemas operacionais.

  - Mantida uma abrangente base de Conhecimento de Vulnerabilidade “KnowledgeBase”. Diariamente são adicionadas novas assinaturas a esta base.

  - Cada scan começa com um módulo de pré-scan, que são as impressões digitais. A impressão digital é feita através do envio de uma série de pacotes especialmente criados para o acolhimento e interpretação dos resultados. Esse scan é capaz de identificar o sistema operacional da máquina, serviços executados e as portas abertas (0-65535). Uma vez que esta informação tenha sido capturada, o mecanismo de verificação seleciona apenas as vulnerabilidades apropriadas, e interpreta os resultados.

- Além de testar os serviços de rede, é capaz de verificar se existe algum tipo de código malicioso utilizando o seu servidor, SNMP, identificação de firewall existente no Servidor, vulnerabilidade de (Dos) negação de serviço, vulnerabilidades de banco de dados remoto, entre outros testes.

- Teste de Penetração (Mini – Pentest)

    - Identifica vulnerabilidades básicas que não são analisadas por ferramentas automatizadas, tendo em vista suas características particulares. Através dos testes desenvolvidos pela equipe da Site Blindado, são pontuados à aderência da aplicação web sete pontos específicos que frequentemente tem sua proteção negligenciada e podem ser explorados para a identificação de falhas e realização de ataques. São eles:

        - 1) Métodos HTTP permitidos – Verifica quais são os Methods que estão ativos no Servidor (TRACE, PUT, DELETE, COPY);

        - 2) Cross Site Scripting – São feitos testes complementares aos automatizados;

        - 3) Blind Sql Injection – São feitos testes complementares aos automatizados;

        - 4) Sql Error – São feitos testes complementares aos automatizados;

        - 5) SSL – Verifica se mesmo instalado o certificado consegue força para entrar sem HTTPS;

        - 6) Área de administração – Verifica se é facilmente localizada a área de administração do cliente;

        - 7) Diretórios descoberto - Verifica se existem diretórios da aplicação e se são passiveis de cópia.

Amazon

- Possui certificado ISO 27001 e PCI, que atestam a segurança nos processos seguidos pela empresa, descritos na seção 3.2. A empresa disponibiliza ao público sua metodologia de testes e segurança através do site: https://aws.amazon.com/pt/compliance/

Testes de funcionamento e monitoramento do site (intranet e plataforma de clientes)

- Runscope (www.runscope.com): com o Runscope é possível medir de forma automatizada a disponibilidade e responsividade do serviços e criar alertas em caso de falhas.

- Boundary (http://www.bmcsoftware.com.br/truesight): utilizado para monitorar o consumo dos recursos de infraestrutura para cada servidor na

nuvem. Alertas são gerados quando o consumo passa dos limites de 80% do consumo de CPU, 40% do consumo de memória e 20% do consumo de escrita em disco.

- Botmetric (https://www.botmetric.com) - A Botmetric possui um plano de auditoria nos nossos sistemas. Neste plano está incluso testes diários de Segurança nos recursos da Warren na nuvem. Nos testes são avaliados possíveis brechas de segurança e a configuração de servidores expostos publicamente.

- Detectify (https://www.detectify.com) - A Detectify realiza testes diários de Segurança de Informação nos recursos da Warren na nuvem. Diariamente, os sistemas da Detectify escaneiam as maquinas em busca de brechas de segurança. As buscas testam mais de 500 vulnerabilidades, incluindo o TOP TEN da OWASP.

4. PROPRIEDADE INTELECTUAL

Todos os documentos desenvolvidos na realização das atividades da Warren ou a elas diretamente relacionados, tais quais sistemas, arquivos, modelos, metodologias, fórmulas, projeções, relatórios de análise, dentre outros, são de propriedade intelectual da Warren.

A utilização e divulgação de qualquer bem sujeito à propriedade intelectual da Warren dependerá de prévia e expressa autorização por escrito do Gerente de Compliance.

Uma vez rompido com a Warren o vínculo do Colaborador, este permanecerá obrigado a observar as restrições ora tratadas, sujeito à responsabilização nas esferas civil e criminal.

5. ESPECIFICIDADES DOS MECANISMOS DE CONTROLES INTERNOS

A Warren, por meio do Gerente de Compliance, mantém disponível, para todos os Colaboradores, quaisquer diretrizes internas, que devem ser sempre respeitadas, podendo atender, entre outros, os seguintes pontos:

i. Definição de responsabilidades dentro da Warren;

ii. Segregação das atividades atribuídas aos integrantes da Warren de forma que seja evitado o conflito de interesses, bem como meios de minimizar e monitorar adequadamente áreas identificadas como de potencial conflito da espécie;

iii. Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da empresa;

iv. Existência de canais de comunicação que assegurem aos Colaboradores, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;

v. Contínua avaliação dos diversos riscos associados às atividades da empresa; e

vi. Acompanhamento sistemático das atividades desenvolvidas, de forma que se possa avaliar se os objetivos da Warren estão sendo alcançados, se os limites estabelecidos e as leis e regulamentos aplicáveis estão sendo cumpridos, bem como assegurar que quaisquer desvios identificados possam ser prontamente corrigidos.

Adicionalmente, serão disponibilizados a todos os Colaboradores equipamentos e softwares sobre os quais a Warren possua licença de uso, acesso à internet, bem como correio eletrônico interno e externo com o exclusivo objetivo de possibilitar a execução de todas as atividades inerentes aos negócios da Warren. A esse respeito, o Gerente de Compliance poderá disponibilizar a diretriz para utilização de recursos de tecnologia, detalhando todas as regras que devem ser seguidas por todo e qualquer Colaborador, independentemente do grau hierárquico dentro da Warren.

São realizados testes periódicos de segurança para garantir a efetividade dos controles internos mencionados neste Manual de Compliance, inclusive em relação à manutenção da infraestrutura e sistemas de informações da Warren, de modo a assegurar o bom uso das instalações, equipamentos e informações confidenciais da Warren, conforme anexos III e IV. Trimestralmente o Gerente de Compliance emite relatórios de advertências sobre todos colaboradores, sócios e prestadores de serviços a respeito das advertências sobre conduta nos diversos pontos monitorados. O exemplo desse relatório encontra-se no anexo V.

6. PLANO DE CONTINUIDADE DE NEGÓCIOS

A Warren possui um Plano de Continuidade de Negócios de forma a garantir a linearidade das operações, prevendo recursos alternativos e estratégias de continuidade em casos de ocorrências inesperadas. De modo a tornar efetivo o presente Plano, todos os funcionários e colaboradores da Warren devem conhecer as práticas do Plano de Continuidade.

Identificada a interrupção de quaisquer dos recursos essenciais às atividades, os responsáveis pela área de TI devem ser imediatamente comunicados a fim de tomar as providências cabíveis nos termos do Plano de Continuidade de Negócios. Todos os Colaboradores devem possuir os contatos telefônicos e e-mail dos responsáveis pela área de TI, de modo a possibilitar a comunicação da contingência ocorrida e a solução

mais rápida do problema, ou, quando não possível obter uma solução imediata, a opção do fluxo alternativo mais viável.

O serviço de distribuição será 100% online através de plataformas desktop e mobile, e será liderado pelo Diretor Rodrigo Costa Carvalho Leite, que usará um desktop com a seguinte configuração, mesma dos demais membros da Área:

• Processador 3.4 GHz Intel Core i3;

• Sistema operacional Windows;

• Memória 4GB 1333 MHz DDR3;

• Disco Rígido 250GB;

• Placa de vídeo Intel HD Graphics;

• Drive de CD/DVD; e

• Softwares: Microsoft Office.

Em caso de falha de fornecimento de energia, a Warren possui nobreak para suportar o funcionamento do ambiente até que o fornecimento seja reestabelecido, ou em caso de longa interrupção, a utilização do servidor de contingência em nuvem associados aos notebooks permitem a utilização da mesma infraestrutura.

Ainda, contará com a infraestrutura da Warren, qual seja:

Internet: a comunicação é estabelecida através de link com a operadora NET Virtual, com velocidade de 60MB (e link de contingência da operadora Vivo de 30MB).

Servidores: a empresa possui 6 (seis) servidores, a seguir detalhados:

• Servidor de e-mails hospedado no Google Mail;

• Servidor de arquivos hospedado no Google Drive;

• Servidor de impressão com o Google Printer;

• Servidor DNS Route 53 hospedado na Amazon;

• Servidor Windows EC2 hospedado na Amazon;

• Servidor Linux EC2 hospedado na Amazon;

Armazenamento de dados: a empresa faz backups semanais por meio do Dropbox e Google Drive. Também utiliza um armazenamento físico para backup local e um espaço em nuvem na Amazon para backup simultâneo.

Todas as atividades dos Colaboradores são compartilhadas de forma a evitar que a ausência de um colaborador impeça as atividades rotineiras do departamento ou da Warren. São feitos manuais dos sistemas e planilhas proprietárias utilizadas.

Em situações não previstas nos termos do Plano de Continuidade de Negócios e que podem afetar as atividades de departamentos específicos ou atividades da Warren como um todo, será feita a mobilização prioritária de recursos humanos e eventuais aquisições de software ou hardware para manutenção do fluxo de operações da gestora.

7. ATIVIDADES EXTERNAS

Os Colaboradores da Warren não poderão exercer atividades externas remuneradas com exceção daquelas pré-aprovadas pelo Gerente de Compliance, sendo-lhes vedada a participação em quaisquer atividades conflitantes, não só as que conflitem com as atividades exercidas diretamente pelo integrante da Warren como também qualquer atividade em que a Warren esteja envolvida, mesmo que em um ramo de negócio distinto daquele em que o Colaborador trabalhe. É vedada qualquer atividade que fira a lei.

8. TREINAMENTO SOBRE ESTE MANUAL DE COMPLIANCE

A Warren possui um processo de treinamento inicial e um programa de reciclagem contínua dos conhecimentos sobre este Manual de Compliance, aplicável a todos os Colaboradores, especialmente àqueles que tenham acesso a informações confidenciais e/ou participem do processo de decisão de investimento. As atualizações ao treinamento dos Colaboradores serão apresentadas pessoalmente a cada Colaborador.

O processo de treinamento inicial e o programa de reciclagem continuada são desenvolvidos e controlados pelo Gerente de Compliance, e exigem o comprometimento total dos Colaboradores quanto a sua assiduidade e dedicação, de modo que a participação nos treinamentos possui caráter obrigatório.

A periodicidade mínima do processo de reciclagem continuada será anual.

A Warren, por meio do Gerente de Compliance, que será a responsável pela implementação do programa de treinamento, validará o material de curso que será ministrado, com grade horária a ser definida.

ANEXO I – Modelo do "Relatório Anual de Compliance"

RELATÓRIO ANUAL DE COMPLIANCE

Porto Alegre, _____ de janeiro de _____.

Aos Srs., Sócios & Diretores,
Ref.: Relatório Anual de Compliance

Prezados,

Em vista do processo de reciclagem anual das regras, políticas, procedimentos e controles internos da WARREN BRASIL GESTÃO E ADMINISTRAÇÃO DE RECURSOS LTDA. ("Warren"), nos termos do Manual de Regras, Procedimentos e Controle s Internos da Warren ("Manual de Compliance"), e do Artigo 22 da Instrução nº 558, de 26 de março de 2015 da Comissão de Valores Mobiliários ("Instrução CVM 558"), e na qualidade de diretora responsável pela implementação, acompanhamento e fiscalização das regras, políticas, procedimentos e controles internos constantes do Manual de Compliance e da Instrução CVM 558 ("Gerente de Compliance"), informo o quanto segue a respeito do período compreendido entre 1º de janeiro e 31 de dezembro de 20[--].

Por favor, encontrem abaixo: (i) a conclusão dos exames efetuados; (ii) as recomendações a respeito de deficiências e cronogramas de saneamento; e (iii) minha manifestação, na qualidade de responsável por ajustar a exposição a risco das carteiras da Warren, assim como pelo efetivo cumprimento da "Política de Gestão de Riscos" da Warren ("Risk Officer"), a respeito das verificações anteriores e das medidas planejadas, de acordo com o cronograma específico, ou efetivamente adotadas para saná-las.

I. Conclusão dos Exames Efetuados
[●]
II. Recomendações e Cronogramas de Saneamento
[●]
III. Manifestação sobre Verificações Anteriores
[●]

Fico à disposição para eventuais esclarecimentos que se fizerem necessários.

_____
Gerente de Compliance

ANEXO II – Termo de confidencialidade e ciência

Eu, ..., portador da Cédula de Identidade nº ..... e/ou Carteira de Trabalho e Previdência Social nº ..... série ....., declaro para os devidos fins que:

1. Estou ciente da existência do "Código de Ética" da WARREN BRASIL GESTÃO E ADMINISTRAÇÃO DE RECURSOS LTDA." ("Código de Ética" e "Warren", respectivamente) e de todas as políticas internas da Warren, inclusive o "Manual de Regras, Procedimentos e Controles Internos" ("Políticas Internas"), que recebi, li e tenho em meu poder.

2. Tenho ciência do inteiro teor do Código de Ética e das Políticas Internas, do qual declaro estar de acordo, passando este a fazer parte de minhas obrigações como Colaborador (conforme definido no Código de Ética), acrescentando às normas previstas no Contrato Individual de Trabalho, se aplicável, e as demais normas de comportamento estabelecidas pela Warren, e comprometo-me a comunicar, imediatamente, aos sócios-administradores da Warren qualquer quebra de conduta ética das regras e procedimentos, que venha a ser de meu conhecimento, seja diretamente ou por terceiros.

3. Tenho ciência e comprometo-me a observar integralmente os termos da Política de Confidencialidade estabelecida na politica interna da Warren, sob pena da aplicação das sanções cabíveis, nos termos do item 4 abaixo.

4. O não-cumprimento do Código de Ética e/ou das Políticas Internas, a partir desta data, implica na caracterização de falta grave, podendo ser passível da aplicação das sanções cabíveis, inclusive demissão por justa causa, se aplicável. Não obstante, obrigo-me a ressarcir qualquer dano e/ou prejuízo sofridos pela Warren e/ou os respectivos sócios e administradores, oriundos do não-cumprimento do Código de Ética e/ou das Políticas Internas, sujeitando-me à responsabilização nas esferas civil e criminal.

5. Participei do processo de integração e treinamento inicial da Warren, onde tive conhecimento dos princípios e das normas aplicáveis às minhas atividades e da Warren, notadamente aquelas relativas à segregação de atividades, e tive oportunidade de esclarecer dúvidas relacionadas a tais princípios e normas, de modo que as compreendi e me comprometo a observá-las no desempenho das minhas atividades, bem como a participar assiduamente do programa de treinamento continuado.

6. As normas estipuladas no Código de Ética e nas Políticas Internas da Warren não invalidam nenhuma disposição do Contrato Individual de Trabalho, se aplicável, e nem de qualquer outra norma mencionada pela Warren, mas servem de complemento e esclarecem como lidar em determinadas situações relacionadas à minha atividade profissional.

7. Autorizo a divulgação de meus contatos telefônicos aos demais Colaboradores, sendo que comunicarei a Warren a respeito de qualquer alteração destas informações, bem como de outros dados cadastrais a meu respeito, tão logo tal modificação ocorra.

8. Declaro ter pleno conhecimento que o descumprimento deste Termo de Compromisso pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

A seguir, informo as situações hoje existentes que, ocasionalmente, poderiam ser enquadradas como infrações ou conflitos de interesse, de acordo com os termos do Código de Ética e das Políticas Internas, salvo conflitos decorrentes de participações em outras empresas, descritos na “Política de Investimento Pessoal”, os quais tenho ciência que deverão ser especificados nos termos previstos no Código de Ética:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Porto Alegre, ... de ..... de 20..... .

ANEXO III – Modelo do "Relatório mensal de segurança da informação"

Relatório Mensal de Segurança da Informação

Porto Alegre, ___ de ____ de 20__.

1. Login individual: Verificação se o colaborador utilizou outra máquina para fazer login. Ou se houve login de outro colaborador na sua máquina.

Colaborador	Data	Máquina – IP	Login Efetuado	Ok?
colaborador.warren	02/01/20xx	xxxxxxxxxx	colaborador.warren	ok
colaborador.warren	03/01/20xx	xxxxxxxxxx	colaborador.warren	ok
warren.warren	03/01/20xx	xxxxxxxxxx	warren.warren	ok
colaborador.warren	04/01/20xx	xxxxxxxxxx	warren.warren	Atenção
warren.warren	04/01/20xx	xxxxxxxxxx	oi.warren	Atenção

Advertências:

Colaborador	Nº de advertências
colaborador.warren	01
warren.warren	01

2. Controle de Impressões:

Colaborador	Área	Impressora utilizada	Ok?
colaborador.warren	Adm. de Recursos	Adm. de Recursos	Ok
colaborador.warren	Adm. de Recursos	Gestão de Recursos	Atenção
warren.warren	Gestão de Recursos	Adm. de Recursos	Atenção
colaborador.warren	Adm. de Recursos	Adm. de Recursos	Ok
warren.warren	Gestão de Recursos	Gestão de Recursos	Ok
oi.warren	BackOffice	Geral	Ok

Advertências:

Colaborador	Nº de advertências
colaborador.warren	01
warren.warren	01

3. Controles de Acesso

Colaborador	Área	Diretórios que tem acesso	Desde	Acesso de acordo com a área?	Autorização do Diretor da área

colaborador.warren	Adm. de Recursos	Adm. Recursos	XX/XX/XXXX	Sim	Ok
		Manuais e Códigos (Geral)	XX/XX/XXXX	Sim	Ok
		Treinamentos	XX/XX/XXXX	Sim	Ok
		Lâminas e Regulamentos – Fundos	XX/XX/XXXX	Sim	Ok
warren.warren	Gestão de Recursos	Gestão de Recursos	XX/XX/XXXX	Sim	Ok
		Manuais e Códigos (Geral)	XX/XX/XXXX	Sim	Ok
		Treinamentos	XX/XX/XXXX	Sim	Ok
		Lâminas e Regulamentos – Fundos	XX/XX/XXXX	Sim	Ok
		Controle Risco	XX/XX/XXXX	Sim	Ok
oi.warren	Backoffice	BackOffice	XX/XX/XXXX	Sim	Ok
		Manuais e Códigos (Geral)	XX/XX/XXXX	Sim	Ok
		Treinamentos	XX/XX/XXXX	Sim	Ok
		Lâminas e Regulamentos – Fundos	XX/XX/XXXX	Sim	Ok
		Controle Risco	XX/XX/XXXX	Sim	Ok

Árvore de Permissões

/

4. Checklist Desligamento de pessoas:

Colaborador	**Data desligamento**	**Item**	**Status**
wwwwwww	XX/XX/XXX	Exclusão arquivos pessoais	
		Transferência arquivos da área para diretório do Diretor	
		Cancelamento do acesso a sistemas próprios	
		Cancelamento do acesso a sistemas de terceiros	
		Devolução da chave de controle de acesso físico à área	

Total de pessoas desligadas: ____
Irregularidades: ____

5. Backup

Diretório	**Data Backup**	**Arquivos salvos**

6. Resumo Relatório Mensal de Segurança da Informação

Teste	**Total de testes**	**Irregularidades**	**% Irregularidades**
1. Login individual	264	6	2%
2. Controle de Impressões	38	2	5%

3. Controle de Acesso	12	0	0%
4. Desligamentos	01	0	0%
5. Backup	4	0	0%

ANEXO IV – Modelo do “Relatório trimestral de acesso a internet e telefonemas”

Relatório trimestral de monitoramento: acesso à internet e telefonemas

Período: ___ de 20__ a ___ de 20__.

1. Acessos à internet
    - Total de acessos à internet: xx acessos.
    - Total de acessos monitorados (2% do total): xx.
    - Número de advertências: xx
    - Colaboradores que devem ser monitorados mensalmente: xx

Data	Colaborador	Website acessado	Advertência?

2. Ligações telefônicas
    - Total de ligações: xx.
    - Total de ligações monitoradas (2% do total): xx.
    - Número de advertências: xx
    - Colaboradores que devem ser monitorados mensalmente: xx

Data	Colaborador	Destino	Advertência?

ANEXO V – Modelo do "Relatório trimestral de advertências"

Relatório Trimestral de Advertências

Período: ___ de 20__ a ___ de 20__.
Abrangência: o presente relatório inclui todos que possuem algum vínculo com a Warren, especialmente acesso às dependências físicas ou informações internas da organização.

- Total de advertências:

Data	Colaborador	Área	Motivo da advertência

- Colaboradores com mais de 5 advertências: xxxxxxxx

- São motivos de advertências:

1. Transmissão/Divulgação de informações internas sem autorização do Gerente de Compliance;
2. Falta de cuidado e disciplina em relação a documentos impressos (documentos deixados na impressora de forma recorrente);
3. Tentativa de utilização de dispositivos que possibilitem conexão, transmissão ou armazenamento de informações, tais como *hard drives*, *pen-drives*, *disquetes*, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Warren;
4. Tentativa de conexão de equipamentos na rede da Warren sem autorização da Área de Compliance;
5. Envio ou repasse por e-mail de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo;
6. Envio ou repasse de e-mails com opiniões, comentários ou mensagens que possam denegrir a imagem e/ou afetar a reputação da Warren;
7. Tentativa de instalação via internet (*download*) sem autorização da Área de Compliance;
8. Divulgação de informações privilegiadas, conforme capítulo 2.1.2 do Manual de Regras, Procedimentos e controles internos;
9. Prática de *Insider trading*, conforme capítulo 2.1.3 do Manual de Regras, Procedimentos e controles internos;
10. Divulgação de material de propriedade intelectual da Warren sem autorização do *Gerente de Compliance*;
11. Circulação constante em áreas que não são destinadas ao colaborador (especialmente colaboradores das áreas de Administração Fiduciária e Gestão de Recursos).