TRUXT
INVESTIMENTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E CONTINUIDADE DE NEGÓCIOS

TRUXT INVESTIMENTOS LTDA.

Dezembro/2020

ÍNDICE

INTRODUÇÃO

A Política de Segurança da Informação e Cibernética e Plano de Continuidade de Negócios ("Política") da Truxt Investimentos ("Truxt", "Gestora" ou simplesmente empresa), também referida como Política, é o documento que orienta e estabelece as diretrizes corporativas da Truxt para a proteção dos ativos de informação, controles de segurança cibernética e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

A presente Política está baseada nas melhores práticas de mercado para a gestão da segurança da informação, bem como está de acordo com as leis, regulamentação e autorregulamentação vigentes em nosso país, incluindo o Código ANBIMA de Regulação e Melhores Práticas para Administração de Recursos de Terceiros ("Código ANBIMA").

Aplicações da Política

As diretrizes aqui estabelecidas deverão ser seguidas por todos os Colaboradores. A responsabilidade em decorrência desta Política deve ser comunicada no início do vínculo com a Gestora, devendo os mesmos assinar o Termo de Responsabilidade e Confidencialidade, de forma manual ou eletrônica, excetuadas as hipóteses permitidas em lei, na forma do Anexo I ao Manual de *Compliance*.

SEGURANÇA DA INFORMAÇÃO

Controle do Acesso: Todo acesso a diretórios e sistemas de informações da Gestora deve ser controlado. Somente poderão acessar tais diretórios e sistemas de informação os Colaboradores previamente autorizados pela Diretora de *Compliance*.

O controle do acesso a sistemas de informações da Gestora levará em conta as seguintes premissas:

- Garantia de que o nível de acesso concedido ao Colaborador é adequado ao seu perfil; e
- Cancelamento imediato do acesso concedido a Colaboradores desligados, afastados ou que tenham sua função alterada na Gestora.

Barreiras de controle de informações

Os Colaboradores detentores de informações confidenciais ou privilegiadas, em função de seus cargos ou atribuições na Gestora, devem estabelecer uma barreira de informações para os demais Colaboradores. De forma não exaustiva, as seguintes condutas, além das mencionadas no item de Segurança Cibernética abaixo:

- Os Colaboradores devem evitar circular em ambientes externos à Gestora com cópias (físicas ou digitais) de arquivos contendo Informações Confidenciais, salvo se necessárias ao desenvolvimento do projeto e no interesse do cliente, devendo essas cópias ser criptografadas ou mantidas através de senha de acesso;

- O descarte de Informações Confidenciais em meio digital deve ser feito de forma a impossibilitar sua recuperação, sempre com a orientação do superior hierárquico;

- Os Colaboradores devem estar atentos a eventos externos que possam comprometer o sigilo das informações da Gestora, como por exemplo vírus de computador, fraudes, etc.; e

- Assuntos confidenciais não devem ser discutidos em ambientes públicos ou locais considerados expostos.

Identificação dos detentores da informação, manutenção de registros e *logs*

A Diretora de *Compliance* deve manter o registro dos Colaboradores que detenham informações privilegiadas, com a indicação do tipo de informação detida, devendo informar aos Diretores da Gestora todas as informações privilegiadas que estejam em poder dos Colaboradores que possam significar restrição nas operações da Gestora.

Será atribuído a cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que os usuários (*login*) individuais de Colaboradores internos serão de responsabilidade do próprio e os usuários (*login*) de terceiros serão de responsabilidade do diretor da área contratante. Assim, é possível realizar a identificação dos detentores da informação para eventual responsabilização, se for o caso.

A Gestora informa, ainda, que poderá tomar as seguintes medidas:

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação da Diretora de Compliance;
- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade; ou
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da Gestora e sujeitará o usuário às sanções administrativas e legais cabíveis, observado o disposto no Manual de Compliance da Gestora.

Para fins de ilustração, segue uma lista não exaustiva de eventuais exemplos que podem ocasionar sanções: uso ilegal de software; introdução (intencional ou não) de vírus de informática; tentativas de acesso não autorizado a dados e sistemas; ou a divulgação de informações sensíveis da Gestora.

Proteção da Base de Dados

Os recursos computacionais da Gestora devem ser: (i) protegidos contra adulterações; e (ii) permitir a realização de auditorias e inspeções, na linha das regras de Segurança Cibernética abaixo. Todos os registros eletrônicos realizados pela Gestora deverão ser mantidos e estar disponíveis para atender os prazos legais e regulatórios praticados pelos órgãos reguladores locais e de jurisdições que a Gestora atue em mercado regulado.

As informações mantidas em meios eletrônicos devem ser salvas em bases replicadas (*backups*) e devem permanecer íntegras e acessíveis por prazo não inferior a 5 (cinco) anos. O acesso a essas bases deve ser limitado somente a pessoas autorizadas pela área de *Compliance*.

Vazamento de Informações Confidenciais

Os Colaboradores deverão comunicar à área de *Compliance* quaisquer casos de violações às normas de Segurança da Informação que tenham conhecimento. Toda violação ou desvio é investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos. Em caso de vazamento de informação confidencial, a Diretora de

Compliance discutirá com a equipe de TI qual o melhor plano efetivo de recuperação e medidas para minimizar e prevenir danos, levando o assunto à Diretoria, conforme o caso.

Testes de Segurança da Informação e Treinamento

A Gestora realizará testes periódicos de segurança para os sistemas de informações, sem se limitar a, mas em especial, para os meios eletrônicos, no mínimo a cada 12 (doze) meses.

Faz parte do programa de *Compliance* da Gestora a realização de treinamentos iniciais e anuais para seus Colaboradores, ocasião em que serão abordados diversos temas objeto de suas políticas, na linha da Política de Treinamento.

O referido treinamento deverá incluir os tópicos abaixo:

Segurança da Informação

- Confidencialidade
- Barreiras de controle de informações
- Vazamento de informações confidenciais;

Segurança Cibernética

- Ações de prevenção e proteção
- Phishing, incluindo ações de engenharia social
- Email e utilização da internet
- Computadores, dispositivos móveis e outros recursos tecnológicos;

Plano de Contingências

- Eventos/ameaças potenciais
- Plano de respostas a incidentes
- Proteção e recuperação de dados e documentos;

SEGURANÇA CIBERNÉTICA

Objetivos

Estabelecer diretrizes que permitam aos Colaboradores da Truxt seguirem padrões de comportamento relacionados à segurança cibernética adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança cibernética, bem como a implementação de controles e processos para seu atendimento.

Preservar as informações da Truxt quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Esta Política dá ciência a cada Colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Princípios da Política

Toda informação produzida ou recebida pelos Colaboradores como resultado da atividade profissional contratada pela Truxt pertence à referida empresa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos Colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

A Truxt, por meio de sua equipe de TI, supervisionada pela Diretora de *Compliance*, deverá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

Responsável pela Segurança Cibernética

A Diretora de *Compliance* da Truxt será a responsável por esta política e suas revisões, bem como para tratar e responder questões de segurança cibernética dentro da Gestora.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Diretora de *Compliance*, devendo ser observado o procedimento previsto nesta Política em caso de vazamento de informação confidencial ou no Plano em caso de cenário de crise, que inclui falha de segurança cibernética grave.

A Diretora de *Compliance* irá se consultar com o Gerente de TI, tendo como objetivo a supervisão e monitoramento das regras Segurança Cibernética, conforme aqui previsto. A consulta irá ocorrer sempre que necessário, mediante convocação por email.

Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Todos os requisitos de segurança da informação e segurança cibernética, incluindo a necessidade de planos de contingência, serão previamente identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a Gestora julgar necessário para reduzir os riscos dos seus ativos de informação, como, por exemplo, nas estações de trabalho, notebooks, smartphones, nos acessos à Internet, no correio eletrônico, nos sistemas comerciais e financeiros ou por terceiros.

A Truxt exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus Colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Das responsabilidades

Da Gestão de Tecnologia e Segurança da Informação

A Diretora de *Compliance*, enquanto responsável pela presente Política, ou outro Colaborador indicado por esta, com o auxílio da equipe de TI realizará as seguintes atividades:

- Testar a eficácia dos controles utilizados e informará ao CEO os riscos residuais.
- Acordar com o CEO o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.
- Configurar os equipamentos, ferramentas e sistemas concedidos aos Colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política. Segregar as funções administrativas, operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.
- Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a Truxt.
- Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

  A Diretora de *Compliance* deve ser previamente informada sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada.

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.
- Proteger continuamente todos os ativos de informação da Gestora contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.
- Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da gestora em processos de mudança, sendo ideal a proteção contratual para controle e responsabilização no caso de uso de terceiros.
- Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, exigindo o seu cumprimento dentro da Gestora.
- Realizar auditorias periódicas de configurações técnicas e análise de riscos. Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
- Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da gestora.
- Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
- Monitorar o ambiente de TI, gerando indicadores e históricos de:
    - Uso da capacidade instalada da rede e dos equipamentos;
    - Tempo de resposta no acesso à internet e aos sistemas críticos da Truxt;
    - Períodos de indisponibilidade no acesso à internet e aos sistemas críticos

da Truxt;

- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

- Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
- Propor e apoiar iniciativas que visem à segurança dos ativos de informação da Truxt.
- Promover a conscientização dos Colaboradores em relação à relevância da segurança da informação para o negócio da Truxt, mediante campanhas, palestras, treinamentos e outros meios de endomarketing.
- Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Identificação/Avaliação de Riscos (*Risk Assessment*)

A Gestora deverá identificar os riscos internos e externos, bem como os ativos de hardware e software e processos que precisam de proteção. Esse processo será conduzido e documentado pela área de TI.

Após a condução do referido processo, a área de TI deverá discutir com a Diretora de *Compliance* as opções de tratamento a serem adotadas, considerando a seleção de controles para manter os riscos dentro de limites aceitáveis pela Gestora, considerados os possíveis

impactos financeiros, operacionais e reputacionais, em caso de um evento de segurança, assim como a probabilidade do evento acontecer.

Segue abaixo uma lista não exaustiva de alguns riscos de segurança cibernética identificados, na avaliação inicial:

- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de hackers;
- Comunicações falsas utilizando os dados coletados para ter credibilidade e enganar vítimas e comprometimento de estações de trabalho decorrente de cliques em link malicioso ("*Phishing*");
- Exposição do ambiente devido a uma brecha de segurança, por diversos motivos como a instalação de software em contrariedade com as aprovações e condições estabelecidas nesta Política; ou
- Vazamento de informações durante tráfego de dados não criptografados.]

A Gestora deverá revisar o processo de cibersegurança periodicamente com o fim de estabelecer, manter e monitorar a estrutura de governança, assegurando que as atividades de gerenciamento de segurança requeridas sejam executadas corretamente e de forma consistente pelos profissionais designados.

Ações de Prevenção e Proteção

A Gestora estabeleceu um conjunto de medidas buscando mitigar os riscos identificados, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles, na forma abaixo. Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade.

Correio Eletrônico

O objetivo desta Política é informar aos Colaboradores da Truxt quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Truxt é para fins corporativos e relacionados às atividades do Colaborador usuário dentro da empresa. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Truxt e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos Colaboradores o uso do correio eletrônico da Truxt para as seguintes atividades:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da gestora;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Truxt vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando a Truxt estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Truxt;
    - Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador;
    - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs,

.hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Contenha anexo(s) superior(es) a 36 MB para envio (interno e internet) e 37 MB para recebimento (internet);
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos locais ou do país (propaganda política);

Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
Internet

Todas as regras atuais da Truxt visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente

da rede corporativa da empresa com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, a Truxt, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política.

A Truxt, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas.

Toda tentativa de alteração dos parâmetros de segurança, por qualquer Colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Colaborador e ao respectivo superior. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a empresa cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela empresa aos seus Colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos na Truxt.

Como é do interesse da Truxt que seus Colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os Colaboradores que estão devidamente autorizados a falar em nome da Truxt para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os Colaboradores autorizados pela Gestora poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de

Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os Colaboradores com acesso à internet poderão fazer o download somente de programas ligados diretamente às suas atividades na Truxt e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretora de *Compliance*.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela equipe de TI.

Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Truxt para fazer o download ou distribuição de software ou dados não autorizados e não legalizados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de jogos são proibidos.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload de qualquer software licenciado à Truxt ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os Colaboradores não poderão utilizar os recursos da Truxt para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) não serão permitidos. Já os serviços de *streaming* (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos.

Os serviços de email externos e de armazenamento online (Gmail, Hotmail, Dropbox, Google Drive e afins) não serão permitidos, mas poderão ser liberados caso o diretor responsável pela área solicitante requisite formalmente à Diretora de *Compliance*. Ainda que seja possível acessar serviços de comunicação instantânea (ex. Whatsapp), estes não configuram canal de comunicação oficial da Truxt.

O upload de documentos é bloqueado e o envio de informações confidenciais através de serviços de comunicação instantânea (Whatsapp e afins) é vedado. Não é permitido acesso a sites de proxy.

Identificação

Os dispositivos de identificação e senhas protegem a identidade do Colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a Truxt e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os Colaboradores.

Todos os dispositivos de identificação utilizados na Truxt, como o número de registro do Colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a empresa e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um Colaborador, a responsabilidade perante a Truxt e a legislação (cível e criminal) será dos usuários que dele se utilizarem.

É proibido o compartilhamento de login para funções de administração de sistemas.

A Área de Recursos Humanos da Truxt é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos Colaboradores.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres, utilizando caracteres especiais (@ # $ %), letras maiúsculas, letras minúsculas ou números, contendo pelo menos 3 (três) das categorias listadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Diretora de *Compliance* da Truxt.

Deverá ser estabelecido um processo para a renovação de senha.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 120 (cento e vinte) dias, não poderão ser repetidas as 12 (doze) últimas senhas. Será implementada a two-factor authentication para as senhas do Microsoft Office 365 e do VPN para todos os colaboradores.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, a Área de Recursos Humanos deverá imediatamente comunicar tal fato a equipe de TI, a fim de que essa

providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

Caso o Colaborador esqueça sua senha, ele deverá requisitar formalmente a troca, para que a equipe de TI realize o cadastro de uma nova senha.

Computadores e Recursos Tecnológicos

Os equipamentos disponíveis aos Colaboradores são de propriedade da Truxt, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da gestora, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da Diretora de *Compliance* da Truxt, ou de quem este determinar. As áreas que necessitarem fazer testes deverão solicitá-los previamente à Diretora de *Compliance*, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a equipe de TI mediante registro de chamado junto à Diretora de *Compliance*.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da Truxt (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o

armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos Colaboradores da empresa deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os Colaboradores da Truxt e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Diretora de *Compliance*.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de Colaboradores não autorizados. Tais senhas serão definidas pela equipe de TI da Truxt, que terá acesso a elas para manutenção dos equipamentos.
- Os Colaboradores devem informar à Diretora de *Compliance* da Truxt, por meio formal, qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da equipe de TI da Truxt ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização da Diretora de *Compliance*.
- Deve se ter extremo cuidado com o consumo de alimentos e bebidas na mesa de trabalho e próximo aos equipamentos.
- O Colaborador deverá manter a configuração do equipamento disponibilizado pela Truxt, seguindo os devidos controles de segurança exigidos pela Política de Segurança

da Informação e Continuidade de Negócios e pelas normas específicas da gestora.

- Todos os recursos tecnológicos adquiridos pela Truxt devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Dispositivos Móveis

A Truxt deseja facilitar a mobilidade e o fluxo de informação entre seus Colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da empresa, ou aprovado e permitido pela Diretora de *Compliance*, como: notebooks e smartphones.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

A Truxt, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O Colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções na Truxt, mesmo depois de terminado o vínculo contratual mantido com a empresa.

Todo Colaborador deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

Todo Colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs,

sem a devida comunicação e a autorização da Diretora de *Compliance* e sem a condução, auxílio ou presença de um técnico da equipe de TI.

O Colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da equipe de TI da Truxt.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela empresa constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo Colaborador como: sua casa, hotéis, fornecedores e clientes.

O Colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará que assumiu todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a Truxt e/ou a terceiros.

Datacenter

O acesso ao Datacenter somente deverá ser feito por sistema forte de autenticação. Por exemplo: biometria, cartão magnético entre outros.

Todo acesso ao Datacenter, pelo sistema de autenticação forte, deverá ser registrado (usuário, data e hora) mediante software próprio.

Deverá ser executada semestralmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

O usuário "administrador" do sistema de autenticação forte ficará de posse e administração do coordenador de infraestrutura.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada e salva no diretório de rede.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um Colaborador autorizado.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência a qualquer Colaborador responsável pela administração de liberação de acesso.

A chave da porta do Datacenter deverá ficar na posse da Diretora de *Compliance*, ou Colaborador definido por esta.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a autorização da Diretora de *Compliance*.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto famígero ou inflamável.

A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará com o preenchimento da solicitação de liberação pelo Colaborador solicitante e a autorização formal desse instrumento pela Diretora de *Compliance*.

No caso de desligamento de Colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de Colaboradores autorizados.

Monitoramento e Testes

Os mecanismos de supervisão se encontram descritos abaixo, de forma a verificar sua efetividade e identificar eventuais incidentes, detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

O ambiente de TI da Gestora será monitorado, por meio de indicadores e geração de históricos: (i) do uso da capacidade instalada da rede e dos equipamentos; (ii) tempo de resposta no acesso à Internet e aos sistemas críticos da Gestora; (iii) de períodos de indisponibilidade no acesso à Internet e aos sistemas críticos da Gestora; (iv) de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); e (v) das atividade de todos os Colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

A Truxt possui equipe interna de TI especializada para realizar o monitoramento do seu ambiente de rede.

Para garantir as regras mencionadas nesta Política, a Gestora deverá:

- Para os riscos associados a *Phishing*, conduzir treinamentos e campanhas periódicas, bem como testes de *Phishing*,;
- Realizar, a qualquer tempo, inspeção física nas máquinas de hardware;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso; e
- Testar a vulnerabilidade e penetração do Website da Gestora, bem como de todo e qualquer sistema eletrônico desenvolvido internamente pela Gestora, ao menos semestralmente.

Na realização dos testes e monitoramentos aqui referidos, arquivos pessoais salvos em cada computador ou equipamento da Gestora poderão ser acessados, caso a Diretora de Compliance julgue necessário. A confidencialidade dessas informações deve ser respeitada e seu conteúdo será divulgado somente se determinado por decisão judicial.

Plano de Respostas a Incidentes

A Gestora deverá levar em consideração o plano de resposta a incidentes previstos no seu Plano de Continuidade de Negócios abaixo, considerando os cenários de ameaças lá previstos (que inclui falha de segurança cibernética grave) e os descritos abaixo para os demais casos.

Os Colaboradores poderão reportar incidentes diretamente à Diretora de *Compliance*.

Reciclagem e Revisão

A Gestora deverá manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.

Também realizará campanha de conscientização em cibersegurança com o fim de garantir que todos os Colaboradores tenham as habilidades necessárias para proteger as informações como parte de suas responsabilidades por meio do Programa previsto no Manual da Gestora.

PLANO DE CONTINGÊNCIAS

A Gestora desenvolveu e adota um Plano de Contingências ("Plano") como prática essencial de seu dever fiduciário, como objetivo de estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para as atividades da Truxt, em conformidade com as leis, regulamentação e autorregulamentação aplicáveis, em especial a Instrução CVM 558 e o Código ANBIMA. Nesse sentido, a Truxt entende que a prevenção e adequação de sua estrutura não são apenas necessárias, como primordiais de modo a prestar um ótimo serviço de gestão de recursos aos seus clientes.

Eventos/Ameaças potenciais

O Plano traz como principais eventos/ameaças aos negócios da Gestora, cuja lista não tem pretensão de ser exaustiva ou definitiva:

- Baixa conectividade ou perda de conectividade com a internet, falha no sinal ou *hardware* de telecom (incluindo voz) ou na rede de celular;
- Falta de energia (apagão), falta localizada de energia ou falha de circuito / terminal;
- Interrupção dos transportes, greves, protestos ou guerras ou acidentes relevantes;
- Clima extremo, fogo, inundação, explosão, vazamento de gás ou alerta de segurança;
- Invasão sistêmica que prejudique dados internos, incluindo vírus ou ataque de *hackers*;
- Inacessibilidade temporária ou permanente do escritório; ou
- Qualquer outra situação que ameace o ambiente da Gestora, que não descrita acima.

Proteção e recuperação de dados e documentos

Nessa inteligência, com o intuito de garantir a continuidade das atividades da Truxt, é feito o backup das informações digitais e dos sistemas existentes no escritório, através dos seguintes processos:

a) Backup diário realizado na nuvem;
b) Backup diário em disco externo as instalações físicas da Truxt;

c) Manutenção dos sistemas em funcionamento, apesar de falta de energia temporária, através de equipamentos de nobreak instalados para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da Truxt;
d) Manutenção de meios remotos seguros para o trabalho de seus Colaboradores; e
e) Manutenção de servidor reserva.

Plano de Respostas a Incidentes

Procedimento em caso de incidente

Uma vez que o responsável pela segurança cibernética tenha sido acionado devido a um potencial incidente, este deverá atuar em conjunto com a área de TI para solução imediata do problema.

Avaliação Inicial

Na etapa inicial, aspectos e decisões fundamentais deverão ser analisadas e tomadas após o incidente. Deverá ser realizada uma análise do que aconteceu, compreendendo motivos e consequências imediatas, bem como a gravidade da situação, devendo ser decidido a formalização ou não do incidente.

Incidente Caracterizado

Se for caracterizado um incidente, devem ser tomar as medidas imediatas, que poderão abranger (i) se será registrado um boletim de ocorrência ou queixa crime, (ii) se há necessidade de informar à CVM, ANBIMA ou mais alguma autoridade, (iii) se é necessário envolver consultor ou advogado externo; (iv) se haverá comunicação interna ou externa, em especial a Investidor que eventualmente tenha sido afetado; e (v) se houve prejuízo para a Gestora, algum veículo de investimento ou investidor específico. Além disso, caso seja necessário, deverão ser definidos os passos a serem tomados sob o aspecto de cibersegurança, tais como iniciar a redundância de TI, redirecionar as linhas de telefone para os celulares, instruir o provedor de Telecom a desviar linhas de dados/e-mail.

Recuperação

Essa fase começa após o incidente inicial ter sido contornado, já tendo sido a redundância de TI acionada e terceiros-chave notificados, caso necessário. Será realizado um acompanhamento, com um sumário elaborado pelo Responsável pela Segurança Cibernética contendo as medidas a serem tomadas, responsabilidades e prazos.

Quaisquer dados faltando ou corrompidos, ou problemas identificados por Colaboradores da Gestora, devem ser comunicados. Colaboradores externos relevantes deverão ser mantidos atualizados, caso seja necessário.

Retomada

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção. A Área de *Compliance* deverá registrar o histórico em local adequado, como o sistema de gerenciamento.

Ademais, após eventual evento de contingência, a diretora de *Compliance* deverá avaliar os prejuízos decorrentes da ocorrência e propor melhorias e investimentos para a redução dos riscos.

Testes de Contingência

Os Testes de Contingência serão realizados com periodicidade mínima anual ou em virtude das mudanças ocorridas na Gestora que assim o justifiquem, de modo a permitir que a Truxt esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

O objetivo do teste incluirá a avaliação se o Plano desenvolvido é capaz de suportar, de modo satisfatório, os processos operacionais críticos para a continuidade dos negócios da Gestora e manter a integridade, a segurança e a consistência dos bancos de dados criados pela alternativa adotada, e se o Plano pode ser ativado tempestivamente.

Os testes abrangerão os seguintes eventos, apenas de forma amostral, a saber:

a) Testes dos nobreaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;

b) Acesso aos sistemas e aos e-mails remotamente, de endereço externo;
c) Acesso aos dados armazenados externamente; e
d) Outros necessários à continuidade das atividades.

O resultado de cada teste será registrado no documento de Teste de Contingência.

VIGÊNCIA E ATUALIZAÇÃO

Esta Política será revisada em período não superior a 24 (vinte e quatro) meses pela área de *Compliance*, em conjunto com a área de TI, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo, conforme análise e decisão da Diretora de *Compliance*. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.