TRUXT
INVESTIMENTOS

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CONTINUIDADE DE NEGÓCIOS

TRUXT INVESTIMENTOS LTDA.

Maio/2017

ÍNDICE

INTRODUÇÃO

A Política de Segurança da Informação e Continuidade de Negócios da Truxt Investimentos ("Truxt"), também referida como Política, é o documento que orienta e estabelece as diretrizes corporativas da Truxt para a proteção dos ativos de informação 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 recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

OBJETIVOS

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

Nortear a definição de normas e procedimentos específicos de segurança da informação, 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.

APLICAÇÕES DA POLÍTICA

As diretrizes aqui estabelecidas deverão ser seguidas por todos os Colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

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.

É também obrigação de cada Colaborador se manter atualizado em relação a esta Política e aos procedimentos e normas relacionadas, buscando orientação da Diretora de *Compliance* quando não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

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 terceirizada 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.

REQUISITOS DA POLÍTICA

Para a uniformidade da informação, a Política deverá ser comunicada a todos os Colaboradores da Truxt a fim de que a política seja cumprida dentro e fora da empresa.

A Diretora de *Compliance* da Truxt será responsável por prever as regras e normas aqui estabelecidas, bem como a sua revisão.

Tanto a Política quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão da diretora de *Compliance*.

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos Colaboradores. Todos os Colaboradores devem ser orientados sobre os

procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar o Termo de Responsabilidade e Confidencialidade, anexo ao Manual de Compliance da Truxt.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Diretora de *Compliance*.

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, incluindo a necessidade de planos de contingência, devem ser 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.

Esta Política será implementada na Truxt por meio de procedimentos específicos, obrigatórios para todos os Colaboradores, independentemente do nível hierárquico ou função instituição, bem como de vínculo empregatício ou prestação de serviços.

O não cumprimento dos requisitos previstos nesta Política acarretará violação às regras internas da empresa e sujeitará o usuário às sanções administrativas e legais cabíveis.

DAS RESPONSABILIDADES

1 - Da Gestão de Tecnologia e Segurança da Informação

A Diretora de *Compliance*, enquanto responsável pela presente Política de Segurança da Informação e Continuidade de Negócios, ou outro Colaborador indicado por esta, com o auxílio da equipe terceirizada 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.
- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.
- 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.
- Atribuir 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 funcionários serão de responsabilidade do próprio funcionário.
    - Os usuários (login) de terceiros serão de responsabilidade do diretor da área contratante.
- 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.

2 - Do Monitoramento e da Auditoria do Ambiente

Para garantir as regras mencionadas nesta Política, a Truxt poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. A informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- 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;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO

O objetivo desta norma 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 15 MB para envio (interno e internet) e 15 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. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
    - Nome do Colaborador
    - Departamento
    - Nome da empresa
    - Telefone (s)
    - Correio eletrônico

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 de sua Política de Segurança da Informação e Continuidade de Negócios.

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 (baixar) 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 terceirizada de TI.

Os Colaboradores não poderão em hipótese alguma utilizar os recursos da Truxt para fazer o download ou distribuição de software ou dados pirateados, 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 (subida) de qualquer software licenciado a 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 comunicação instantânea (MSN, ICQ e afins) inicialmente não serão permitidos, mas poderão ser liberados caso o Diretor Responsável pela área solicitante requisite formalmente à Diretor de *Compliance*.

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 o 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 que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 8 (oito) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 9 (nove) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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 90 (noventa) dias, não podendo ser repetidas as 12 (doze) últimas senhas. Os sistemas críticos e sensíveis para a empresa e os logins com privilégios administrativos devem exigir a troca de senhas a cada 90 (noventa) dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

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 terceirizada 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 terceirizada 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 terceirizada 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 terceirizada 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 terceirizada 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*.
- É expressamente proibido o consumo de alimentos, bebidas ou fumo 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, smartphones e pendrives.

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.

O suporte da equipe terceirizada de TI aos dispositivos móveis de propriedade da Truxt e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela empresa.

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 terceirizada 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 terceirizada 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 pelo Diretor 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.

PLANO DE CONTINGÊNCIAS

De acordo com seção de requisitos da Política, a presente seção tem o objetivo de estabelecer medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para as atividades da Truxt. 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.

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 no break instalados para suprir o fornecimento de energia nos equipamentos principais para a manutenção das comunicações e atividades mínimas da Truxt;
d) Manutenção de um local externo, em um endereço fora das edificações e instalações físicas da Truxt, onde as atividades poderão ser mantidas no modelo de contingência;
e) Manutenção de meios remotos seguros para o trabalho de seus Colaboradores; e
f) Manutenção de servidor reserva.

Por fim, convém conferir que o local externo que a Truxt utilizará, em caso de contingência, trata-se de uma estrutura compartilhada com outras gestoras de recursos para tratamento de contingências, de forma a agilizar o retorno ao curso normal dos negócios. 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.

1 Testes de Contingência

Os Testes de Contingência serão realizados com periodicidade mínima anual, de modo a permitir que a Truxt esteja sempre aprimorando sua infraestrutura para a continuação de suas atividades.

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

a) Testes dos no-breaks, verificando o status de funcionamento e do tempo de suporte das baterias com carga;
b) Acesso aos sistemas e aos e-mails remotamente, do 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 anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência.