PPSI – Política e Procedimentos de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

Índice

1 – APRESENTAÇÃO

A Política e Procedimentos de Segurança da Informação, também referida como PPSI, é o documento que orienta e estabelece as diretrizes corporativas da Treviso 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 instituição.

A presente PPSI 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.

Com a intenção de aumentar a segurança da infraestrutura tecnológica disponibilizada pela Treviso, seus colaboradores, parceiros e prestadores de serviço em geral, essa PPSI foi, igualmente, desenvolvida visando a orientação geral na área de tecnologia da informação, assim como, ela pretende dispor de uma abordagem educacional para todos aqueles que fazem uso dos ativos de tecnologia da informação disponibilizados.

A Treviso Corretora de Câmbio S/A adota procedimentos no âmbito da Segurança e Tecnologia da Informação com base em princípios e diretrizes que consideram a abordagem baseada no risco inerente à sua atividade cabendo ressaltar que, esta PPSI coaduna com as regras estabelecidas pela Autoridade Reguladora (Banco Central do Brasil) notadamente, a Resolução nº 4.658, de 26 de abril de 2018, a Circular nº 3.909, de 16 de agosto de 2018 e, demais normas que às complementem ou substituam.

Atenciosamente,

Gerência de Tecnologia da Informação

2 – OBJETIVOS

Estabelecer diretrizes que permitam aos colaboradores da Treviso respeitarem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo assegurando, dessa maneira, a capacidade da Treviso para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

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

Atender às normas da Autoridade Reguladora no tocante às premissas de boas práticas na contratação e/ou substituição e utilização de serviços relevantes que incluam *Cloud Computer* (Computação em Nuvem) e, igualmente, Data Center Local.

Estabelecer os procedimentos e os controles adotados para reduzir a vulnerabilidade da Treviso a incidentes e atender aos demais objetivos de segurança cibernética com abrangência, no mínimo, da autenticação, da criptografia, da prevenção e da detecção de intrusão, da prevenção de vazamento de informações, da realização periódica de testes e varreduras para detecção de vulnerabilidades, da proteção contra softwares maliciosos, do estabelecimento de mecanismos de rastreabilidade, dos controles de acesso e de segmentação da rede de computadores e da manutenção de cópias de segurança dos dados e das informações. Referidos procedimentos devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Treviso.

Orientar os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis.

Determinar a realização do registro, da análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Treviso. Referidos registros, análises e controles devem abranger, inclusive, as informações recebidas de empresas prestadoras de serviços a terceiros.

Orientar as diretrizes para:

a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;

b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Treviso, os quais devem, inclusive, contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria Treviso.

c) a classificação dos dados e das informações quanto à relevância; e

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes.

Orientar a instalação dos mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

Sem prejuízo do dever de sigilo e da livre concorrência, estabelecer as iniciativas para compartilhamento de informações sobre os incidentes relevantes, no âmbito de empresas prestadoras de informações, com outras instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil, às quais serão mantidas à disposição daquele Órgão Regulador.

Preservar as informações da Treviso 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 respectivos ativos de tecnologia da informação sempre que necessário.
Base legal: Resolução 4.658, de 26 de abril de 2018, Art. 12º, incisos I e II, alíneas "a","b" e, "c".

3 – APLICAÇÕES DA PPSI

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 PPSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

A aplicação desta PPSI visa assegurar a adoção e a aplicação dos requisitos para contratação de serviços de computação em nuvem, dentro e fora do Brasil, mitigando os incidentes relevantes mediante o registro, a análise da causa e do impacto e, o controle dos efeitos dos incidentes, com vistas à mitigação ou inibição da possibilidade dos incidentes voltarem a ocorrer impactando as atividades da Treviso.

4 – PRINCÍPIOS DA PPSI

Esta PPSI é formulada com base em princípios e diretrizes que buscam assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Treviso pertence à referida instituição. As exceções devem ser explicitadas 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 Treviso, por meio da Gerência de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

5 – REQUISITOS DA PPSI

Para a uniformidade da informação, a PPSI deverá ser comunicada à todos os colaboradores da Treviso a fim de que a política seja cumprida dentro e fora da empresa.

Considerada a atual estrutura organizacional, é atribuída ao Comitê Diretivo a função de comitê multidisciplinar responsável pela gestão dos temas relacionados à segurança da informação, analisando e deliberando as questões tipicamente atribuídas e designadas ao Comitê de Segurança da Informação mediante apontamentos e encaminhamento dos temas e demandas relevantes formuladas e submetidas pela Gerência de Tecnologia da Informação para análise e deliberação do Comitê Diretivo.

Tanto a PPSI quanto as normas deverão ser revisadas anualmente e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise da Gerência de Tecnologia da Informação, que à formulará e submeterá ao Comitê Diretivo para aprovação.

Quando necessário e, para atender demandas e necessidades pontuais da Treviso com suas contrapartes (empresas e pessoas externas à Treviso), deverá constar nos contratos, uma Cláusula de Confidencialidade ou a formalização (assinatura) de um Termo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores. Todos os colaboradores são instruídos e orientados sobre os procedimentos de segurança, bem como do uso correto dos ativos de informação, a fim de reduzir possíveis riscos. Para tanto o aspecto “responsabilidade” e “confidencialidade” tratado nesta PPSI coaduna as disposições do “Código de Ética e Conduta” (vide item 8 e 37, do Código de Ética e Conduta) exigindo, dos colaboradores, a assinatura do termo de responsabilidade.

Todo incidente que afete a segurança da informação deverá ser comunicado inicialmente à Gerência de Tecnologia da Informação e ela, se julgar necessário, deverá encaminhar posteriormente ao Comitê Diretivo para análise e deliberação.

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 instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico, nos sistemas comerciais e financeiros desenvolvidos pela Treviso ou por terceiros.

Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento, testes e homologação.

A Treviso 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 PPSI é implementada na Treviso por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PPSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

6 – DAS RESPONSABILIDADES ESPECÍFICAS

6.1. – Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar à Treviso e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2. – Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto nesta PPSI concebida pela Gerência de Tecnologia da Informação e aprovada pelo Comitê Diretivo.

A concessão de acesso aos ativos de informação poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco

relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições aqui definidas.

6.3. – Dos Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PPSI da Treviso.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da Treviso.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Termo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender esta PPSI.

6.4. – Dos Custodiantes da Informação

6.4.1. – Da Área de Tecnologia da Informação

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes. Bem como garantir a conformidade à regulamentação vigente, observando condições e prazos estipulados nas normas regulatórias.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PPSI, e pelas Normas de Segurança da Informação complementares.

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.

Segregar as funções administrativas, operacionais e educacionais 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, incluindo o ambiente educacional, 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 Treviso.

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

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 (*logins*) individuais de funcionários serão de responsabilidade do próprio funcionário.

- os usuários (*logins*) de terceiros serão de responsabilidade do gestor da área contratante.

Proteger continuamente todos os ativos de informação da empresa 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 empresa em processos de mudança, sendo ideal a auditoria de código e 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, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.

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 empresa.

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 Treviso;
- períodos de indisponibilidade no acesso à internet e aos sistemas críticos da Treviso;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, dentre outros)
- 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);

6.4.2. – Da Gerência de Tecnologia da Informação

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 Treviso.

Publicar e promover as versões da PPSI e as Normas de Segurança da Informação aprovadas pelo Comitê Diretivo.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da Treviso Corretora, mediante campanhas, palestras, treinamentos e outros meios.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

Analisar criticamente, em conjunto com o Comitê Diretivo, os incidentes pertinentes à segurança da informação.

Apoiar o Secretário do Comitê Diretivo na formulação das atas e os resumos das reuniões do Comitê Diretivo, no desenvolvimento dos temas relacionados à Gerência de Tecnologia da Informação, destacando os assuntos que exijam intervenção do próprio comitê ou de outros membros da diretoria.

Manter comunicação efetiva com o Comitê Diretivo sobre assuntos relacionados ao tema que afetem ou tenham potencial para afetar a Treviso.

Buscar alinhamento com as diretrizes corporativas da instituição.

6.4.3. – Do Comitê de Segurança da Informação

A Treviso, por sua estrutura organizacional, recorre ao Comitê Diretivo que recepciona, analisa e delibera sobre os assuntos relacionados à Segurança da Informação.

Portanto, as questões comumente atribuídas à um Comitê de Segurança da Informação, numa estrutura organizacional diferente, na Treviso, são tratadas e é atribuição do Comitê Diretivo constituído por Diretores e Superintendentes os quais, quando necessário, são apoiados por gerentes, assessores e colaboradores com nível hierárquico de supervisão, convidados para participar do Comitê para apoiar tecnicamente o entendimento e as discussões dos temas relacionados às suas áreas de atuação.

Deverá a Gerência de Tecnologia da Informação fazer incluir temas de sua área na pauta do Comitê Diretivo, formalmente, pelo menos uma vez a cada seis meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para a Treviso.

A Gerência de Tecnologia da Informação poderá utilizar especialistas, internos ou externos, para apoiarem nos assuntos que exijam conhecimento técnico específico.

Cabe à Gerência de Tecnologia da Informação submeter ao Comitê Diretivo:

- proposta de investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- proposta de alterações nas versões da PPSI e a inclusão, a eliminação ou a mudança de normas complementares;
- avaliar os incidentes de segurança e propor ações corretivas;
- definir as medidas cabíveis nos casos de descumprimento da PPSI e/ou das Normas de Segurança da Informação complementares submetendo-as ao Comitê para deliberação.

6.5. – DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PPSI, bem como de sua versão educacional, a Treviso 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 do Comitê Diretivo;
- 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.

Em atendimento da norma reguladora, a Treviso instituirá mecanismos de acompanhamento e de controle com vistas a assegurar a implementação e a efetividade dessa PPSI, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, incluindo:

I - a definição de processos, testes e trilhas de auditoria;

II - a definição de métricas e indicadores adequados; e

III - a identificação e a correção de eventuais deficiências.

As notificações recebidas sobre a subcontratação de serviços relevantes serão consideradas na definição desses mecanismos e, referidos mecanismos serão submetidos a testes periódicos pela auditoria interna, quando aplicável, compatíveis com os controles internos da Treviso.

7 – CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores da Treviso quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico da Treviso é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a Treviso e também não cause impacto no tráfego da rede e esteja, sempre, apoiado na ciência e autorização do supervisor imediato do colaborador.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Treviso com o propósito de:

• enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas ao uso legítimo da instituição;

• 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 aquele autorizado a utilizar;

• enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Treviso e suas unidades vulneráveis 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 qualquer uma das unidades da Treviso 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 Treviso;
- ✓ **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 10MB para envio (interno e internet) e 10 MB para recebimento (internet)
- ✓ **tenha** conteúdo considerado impróprio, obsceno ou ilegal;
- ✓ **seja** de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, meaçador, 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
• Gerência ou departamento
• Nome da empresa
• Telefone(s)
• Correio eletrônico

8 – INTERNET

Todas as regras atuais da Treviso 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 instituição 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 Treviso, 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 instituição, 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 PPSI.

A Treviso, 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 gestor. 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 instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades e esteja, sempre, apoiada na ciência e autorização do supervisor imediato do colaborador.

Como é do interesse da Treviso 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 Treviso 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 instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, observando e respeitando as diretrizes dessa PPSI, à Lei de Direitos Autorais e, 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.

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 Gerência de Tecnologia da Informação.

Os colaboradores não poderão sob qualquer hipótese utilizar os recursos da Treviso para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

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 para a Treviso 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 Treviso 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. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerencia de Tecnologia da Informação. Não é permitido acesso a sites de proxy.

9 – 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 Treviso 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 Treviso, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos devem estar associados a uma pessoa física e vinculados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

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

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

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

O Departamento de Recursos Humanos da Treviso é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Tecnologia da Informação responde pela criação da identidade lógica dos colaboradores da Instituição, sempre à luz desta PPSI, do Código de Ética e Conduta e todos os documentos (Políticas, Manuais, Procedimentos, Códigos, Comunicados, etc.) oficiais da Treviso, notadamente, aqueles que endereçam tratamento ou fazem referência aos temas relacionados ao parque tecnológico e à segurança da informação da Treviso.

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 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) 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 Gerência de Tecnologia da Informação da Treviso.

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo com regularidade, principalmente, no caso de suspeita de que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 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, quando da demissão de qualquer usuário, o Departamento de Recursos Humanos deverá, imediatamente, comunicar tal fato ao Departamento de Tecnologia da Informação que bloqueará os acessos. A mesma conduta se aplica aos usuários cujo contrato de 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 registrando pedido via mensagem e-mail endereçada a: suporte@trevisocc.com.br.

10 – COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponibilizados aos colaboradores são de propriedade da Treviso, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações e diretrizes constantes nesta PPSI e nos procedimentos operacionais aqui definidos.

É proibido todo e qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o prévio conhecimento e o acompanhamento de um técnico da Gerência de Tecnologia da Informação da Treviso, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Tecnologia da Informação, responsável jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser realizadas 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 no funcionamento das ferramentas tecnológicas, deverá acionar a Gerência de Tecnologia da Informação mediante registro de chamado no "*service desk*" (envio de mensagem e-mail endereçada a: suporte@trevisocc.com.br).

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 Treviso (fotos, músicas, vídeos, etc.), não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso seja identificada a existência desses arquivos, eles serão excluídos definitivamente, o gestor/supervisor do colaborador será informado e instruído para adotar as medidas disciplinares cabíveis com registro no prontuário do usuário, que deverá arquivado na Gerência de Recursos Humanos cabendo à esta última orientar as medidas disciplinares no caso de reincidência.

Documentos imprescindíveis para as atividades dos colaboradores da instituição 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 Treviso 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 Gerência de Tecnologia da Informação.

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

• Todos os computadores de uso individual deverão ter senha de Bios para restringir os acessos não autorizados. Tais senhas serão definidas pela Gerência de Tecnologia da Informação da Treviso, única responsável habilitada às senhas para manutenção dos equipamentos.

• Os colaboradores devem informar ao departamento técnico 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 Gerência de Tecnologia da Informação da Treviso ou por terceiros devidamente contratados para o serviço.

• Todos os eventuais modems internos ou externos serão 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 dos gestores das áreas e da Gerência de Tecnologia da Informação.

• 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 Treviso, respeitando as regras de segurança exigidas por esta PPSI e pelas demais normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

• Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.

• Todos os recursos tecnológicos adquiridos pela Treviso Corretora 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.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Treviso:

• Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

• Burlar quaisquer sistemas de segurança.

• Acessar informações confidenciais sem explícita autorização do proprietário.

• Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).

• Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

• Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

• Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

• Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

11 – DISPOSITIVOS MÓVEIS

A Treviso restringe o fluxo de informação entre seus colaboradores. Por isso, não permite que eles usem equipamentos portáteis.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Tecnologia da Informação, 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 Treviso, na qualidade de proprietária dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança, inclusive, porém, não limitada à inspeção para validação e aderência das regras contidas nesta PPSI.

O colaborador, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, 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 Treviso, mesmo depois de terminado o vínculo contratual mantido com a instituição.

O suporte técnico aos dispositivos de propriedade da Treviso e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela instituição.

Todo colaborador deverá utilizar senhas de bloqueio automático para os dispositivos em uso e, no caso de “desktop” (computador de mesa), quando das súbitas ausências de suas estações de trabalho.

Não será permitida, sob qualquer hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a necessária comunicação prévia e a expressa autorização da área

responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Tecnologia da Informação.

O colaborador é responsável por manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência de Tecnologia da Informação da Treviso.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição 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.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela Treviso, notificar imediatamente seu gestor direto e a Gerência de Tecnologia da Informação. Este deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

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

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Treviso Corretora deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Tecnologia da Informação.

Equipamentos portáteis, como smart phones, palmtops, pendrives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

12 – CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Assegurar que a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, quer seja no país ou no exterior, atendam às políticas, estratégias e estruturas para o gerenciamento de riscos previstas na regulamentação em vigor, especificamente no tocante aos critérios de decisão quanto à terceirização desses serviços devendo, previamente à sua contratação, contemplar procedimentos tais como:

I - a adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos inerentes; e

II - a verificação da capacidade do potencial prestador de serviço de assegurar:

a) o cumprimento da legislação e da regulamentação em vigor;

b) o acesso da Treviso Corretora de Câmbio S/A aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

c) a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

d) a sua aderência a certificações, exigidas pela Treviso, para a prestação do serviço a ser contratado;

e) o acesso da Treviso aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;

f) o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) a identificação e a segregação dos dados dos clientes da Treviso por meio de controles físicos ou lógicos;

h) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Treviso.

Ressalta-se que, na avaliação da relevância do serviço a ser contratado, a Treviso terá em consideração a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação dos dados e das informações quanto à relevância.

Os procedimentos elencados acima (alíneas de “a” à “h”) estarão presentes nos documentos que formalizam a contratação dos serviços, assim como, aqueles que contemplem a execução de aplicativos por meio da internet, ou aqueles adquiridos pela Treviso, assegurando-se que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

A Treviso utilizará os recursos e as competências necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso de recursos providos nos termos da alínea "f", acima.

Alinhada com a Autoridade Reguladora, a Treviso considera que os serviços de computação em nuvem abrangem a disponibilidade, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I - processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à Treviso implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Treviso ou por ela adquiridos;

II - implantação ou execução de aplicativos desenvolvidos pela Treviso, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;

Ou

III - execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A Treviso é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

Conforme estabelece a regulamentação em vigor, os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem devem ser previamente comunicados ao Banco Central do Brasil.

A comunicação deve conter as seguintes informações:

I - a denominação da empresa a ser contratada;

II - os serviços relevantes a serem contratados; e

III - a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados, no caso de contratação no exterior.

A comunicação será realizada, no mínimo, sessenta dias antes da contratação dos serviços.

As alterações contratuais que impliquem modificação das informações mencionadas nos incisos de I a III, acima, serão comunicadas ao Banco Central do Brasil, no mínimo, sessenta dias antes da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior observarão os seguintes requisitos:

I - a existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;

II - a Treviso assegurará que a prestação dos serviços prestados no exterior não cause prejuízos ao seu regular funcionamento nem embaraço à atuação do Banco Central do Brasil;

III - a Treviso definirá, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e

IV - a Treviso irá prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio, conforme mencionado na alínea I, acima, a Treviso solicitará autorização do Banco Central do Brasil para a contratação, observando o prazo e as informações requeridas para comunicação àquela autarquia.

Para atendimento aos incisos II e III, acima, a Treviso irá assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso da Treviso e do Banco Central do Brasil aos dados e às informações. A comprovação do atendimento aos requisitos mencionados nos incisos I e IV, acima, e o cumprimento da exigência de comunicação com sessenta dias de antecedência, estarão documentados por meio de instrumentos

próprios e, os contratos para a prestação de serviços relevantes de processamento e armazenamento de dados e computação em nuvem devem prever:

I - a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II - a adoção de medidas de segurança para a transmissão e armazenamento dos dados citados no inciso I, anterior;

III - a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

IV - a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados citados no inciso I ao novo prestador de serviços ou à instituição contratante; e
b) exclusão dos dados citados no inciso I pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a", anterior, e a confirmação da integridade e da disponibilidade dos dados recebidos;

V - o acesso da Treviso a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento do disposto nos incisos I a III (anteriores);

b) informações relativas às certificações e aos relatórios de auditoria especializada; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VI - a obrigação de a empresa contratada notificar a Treviso sobre a subcontratação de serviços relevantes necessários para a entrega dos serviços contratados;

VII - a permissão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;

VIII - a adoção de medidas pela Treviso, em decorrência de determinação do Banco Central do Brasil; e

IX - a obrigação de a empresa contratada manter a Treviso permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor. O contrato acima mencionado irá prever, para o caso da decretação de regime de resolução da Treviso pelo Banco Central do Brasil:

I - a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das

informações, bem como aos códigos de acesso, citados no inciso VII, anterior, que estejam em poder da empresa contratada;
e

II - a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da Treviso na qualidade de contratante.
Base legal: Art. 11º a 17º, da Resolução 4.658, de 26 de abril de 2018.

13 – DATACENTER - PROCEDIMENTOS

Base legal: Art. 11º, da Resolução 4.658, de 26 de abril de 2018.

13.1 – O acesso ao Datacenter Local somente deverá ser feito por biometria, cartão magnético entre outros conhecidos desde que, previamente, autorizados pela Gerência de Tecnologia da Informação.

Contingencia

A TREVISO disponibiliza recursos que permitem acesso ao ambiente de sistema, em produção, para até 50 colaboradores, de forma remota, via acesso seguro (VPN), possibilitando a realização das atividades atribuídas desde suas residências ou de qualquer computador disponível, conectado à internet.

A TREVISO conta com opções de sites remotos (residências e/ou escritórios alugados), utiliza ferramentas tecnológicas tais como; webmail e celulares, cujo serviço de e-mail e acesso remoto à rede, protegido por criptografia forte, permite aos funcionários e colaboradores a realização de suas tarefas, fora do ambiente do escritório matriz.

Instalações Corporativas da TREVISO

As instalações da TREVISO, no endereço matriz, estão localizadas no Condomínio Juscelino Kubitscheck que é provido de equipes técnicas, formadas em engenharia, treinadas periodicamente. O treinamento contempla exercício periódico de abandono da edificação, utilizando-se rotas de fuga e apoio da defesa civil, todos em alerta e funcionamento 24h x 7d. Em obediência a regra vigente, a Treviso dispõe de dois brigadistas que compõem a equipe condominial interna especialmente designada para atuar nas situações de emergência.

Acesso a TREVISO

O Condomínio Juscelino Kubitscheck dispõe de um corpo de segurança em atividade alerta 24 horas. O acesso dos visitantes aos escritórios somente é permitido mediante identificação com registro em foto e apresentação de documento de identidade válido, na recepção localizada no piso térreo. O acesso aos escritórios somente é liberado após

autorização da TREVISO (condômino), munido de crachá eletrônico que permite acesso exclusivo aos elevadores.

O acesso ao escritório da TREVISO é exclusivo pela recepção, necessariamente na presença de um colaborador que acompanha o visitante durante sua permanência no espaço corporativo. Aos colaboradores, o acesso ao escritório da Treviso é controlado por sistema de monitoramento de acesso eletrônico, por Biometria e dispositivo eletromagnético e, o acesso aos equipamentos críticos somente é permitido aos colaboradores que atuam na área de Tecnologia e Segurança da Informação.

Visando a segregação de funções e o combate ao conflito de interesse, as salas das equipes de Cadastro, Análises de Clientes, Prevenção à lavagem de dinheiro e ao financiamento do terrorismo e, Tecnologia e Segurança da Informação, têm acesso restrito permitido somente aos funcionários e colaboradores de cada departamento mediante senha em dispositivo eletrônico para acionamento de trava eletromagnética.

Serviços críticos para as atividades da TREVISO

A TREVISO considera o fornecimento de energia elétrica como serviço crítico para suas atividades. Por essa razão, no endereço sede, a TREVISO dispõe de equipamentos de nobreak de 60 KVA, para os servidores, o qual é acionado automaticamente no caso de interrupção no fornecimento de energia.

13.2. – A Treviso contratou e faz uso do serviço de “hospedagem de servidores” junto a RTM. Todo acesso ao Datacenter RTM (Cloud) é realizado pelo sistema de autenticação forte que registra (usuário, data e hora) mediante software próprio.

Infraestrutura da RTM

Seguindo conceitos de infraestrutura, os detalhes foram pensados para oferecer segurança e alta disponibilidade necessárias para a criticidade da operação, garantindo redundância em seus principais componentes.

A RTM está localizada em endereços estratégicos nos centros das cidades de São Paulo e Rio de Janeiro, permitindo acessibilidade rápida e fácil às suas instalações por variados modais de transporte e disponibilidade de estacionamentos, hotéis e restaurantes nas proximidades.

Conectividade

A RTM está conectada às principais operadoras de telecomunicações do Brasil, proporcionando qualidade e agilidade nos serviços prestados devido ao comprometimento alcançado através da parceria e ótimo relacionamento focado no melhor atendimento ao mercado financeiro.

A RTM dispõe de uma rede estruturada para serviços de dados, voz e vídeo, que conecta através da tecnologia IP/MPLS a maioria das instituições financeiras a provedores de serviço e informação, incluindo seus Sites de Contingência e Datacenters. Esta rede é totalmente monitorada e acompanhada por um sistema de controle de tráfego.

Energia

As instalações da RTM possuem sistemas de alimentação de energia redundantes em uma rede estabilizada que trabalham com autonomia garantida por nobreaks e geradores.

Refrigeração

A RTM está instalada em edifícios com sistemas de refrigeração centrais contingenciados por sistemas de refrigeração próprios. As áreas dos datacenters são mantidas em constante estado de refrigeração e umidade, estabilizadas e controladas eletronicamente em regime de 24x7x365.

Extinção de Incêndio

Todas as áreas da RTM possuem sistemas de detecção e combate à incêndio, que acionam automaticamente as equipes responsáveis e outros procedimentos padrões descritos. Projeto de extinção de incêndio via sistema de gás, disponível, com custos e prazos definidos exclusivamente para as áreas dos datacenters.

Segurança

A RTM possui um esquema de segurança que restringe e controla o acesso às principais dependências da empresa. Utiliza sensores de entrada e arrombamento em todas as portas externas, e detecção de presença nas principais salas e áreas de circulação. Complementarmente, possui monitoramento por câmeras com gravação.
O sistema de segurança está conectado em tempo integral a uma central, com disparo programado para uma empresa de segurança particular, delegacias de polícia da região, pessoas chave da RTM e encarregados da segurança do Condomínio.
Além do seu sistema privado, a RTM conta com a segurança 24x7x365 dos edifícios, composto por guardas, detectores de presença e monitoramento por câmeras, conectados à Segurança Central do Condomínio.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, é providenciada, imediatamente, a sua exclusão do sistema de autenticação forte e da lista de colaboradores autorizados (RTM), procedimento este sob a incumbência da Superintendência Administrativa quando se tratar do datacenter local.

14. - CONTINGÊNCIAS DE INFRAESTRUTURAS TECNOLÓGICAS

Base legal: Art. 3º, da Resolução 4.658, de 26 de abril de 2018

14.1. - ESTRUTURA DISPONIBILIZADA

Total NetWork Monitor:

Software de gerenciamento e controle de ativos da TREVISO, baseado em metodologia ITIL – *Information Technology Infrastructure Library*.

Suas características são:

a) Gerenciamento de Servidores - Falhas, desempenho, serviços e auditoria da operação da gerência.

- Gerenciamento da operação baseado em serviços;
- Visualização gráfica do impacto que os eventos causam nos negócios;
- Detecção da causa raiz através da modelagem de serviços;
- Gerenciamento de performance e disponibilidade integradas;
- Gerenciamento do ambiente heterogêneo;
- Solução distribuída que monitora, controla e reporta a saúde do ambiente de TI;
- Visão única do ambiente gerenciado;
- Interface única.

b) Gerenciamento de Falhas de Redes:

- Gerenciamento de ambientes switch nível 2 e router nível 3;
- Interface web com uma visão dinâmica;
- Possibilidade de gerenciamento de eventos facilitando o conhecimento da causa raiz;
- Coleta de informações sobre a rede ajudando na identificação de problemas;
- Gerenciamento pró-ativo;
- Acesso remoto via Web;
- Monitoração dos tempos de resposta dos caminhos da rede;
- Análise dos caminhos da rede baseado nas aplicações e protocolos;
- Diagnóstico e latência dos caminhos estáticos e dinâmicos da rede;
- Relatórios atuais e históricos com as informações dos caminhos da rede;
- Visualização gráfica dos caminhos da rede.

c) Gerenciamento de Performance de Redes:

- Relatórios com informações para garantir a disponibilidade e máxima utilização dos recursos de rede;
- Relatórios técnicos/gerenciais com informações atuais;
- Identificações de como os elementos da rede afetam o desempenho;
- Geração de relatórios do status do desempenho da rede.

14.2. - SITUAÇÕES DE CONTINGÊNCIA PREVISTAS

14.2.1. - Falha no Sistema de Telecom

a) Abrangência:

Operadora de telefonia fixa SP, operadora de celular, central SP*, link* de *Internet* e *links* diversos

b) *Contingências existentes:*

- Para as centrais telefônicas: linhas fixas diretas, fora das referidas centrais, disponíveis para os usuários da TREVISO, inclusive para fax, aparelhos celulares corporativos utilizados por colaboradores com itens adicionais disponíveis no Apoio, igualmente, os aparelhos celulares pessoais dos usuários;

- Para operadoras de telefonia fixa e centrais telefônicas: como contingência de *link*, tanto no *site* de contingência e da Matriz, utiliza-se duas operadoras de telefonia fixa. Caso a infraestrutura de uma das operadoras esteja indisponível, as ligações dos usuários serão roteadas automaticamente pelo *link* da operadora que estiver disponível. Para as centrais telefônicas, dispomos de aparelhos celulares disponíveis com colaboradores e itens adicionais disponíveis no Apoio, igualmente, os aparelhos celulares pessoais dos usuários;

- Para *link* Internet contamos com 5 links de internet de diferentes meios Físicos/Operadoras, por exemplo, Fibra Ótica, Rádio e Banda Larga, operando simultaneamente, gerenciados por um firewall que, ao reconhecer queda ou falha de algum deles, imediatamente, o desabilita e emite alarme.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Ativação da contingência em caso de falha de *hardware* e/ou *software*:

A equipe de TI-Infra informará aos usuários sobre a queda dos sistemas de telefonia, orientando-os a utilizar as linhas diretas existentes e/ou os celulares. Caso a contingência tenha sido decorrente de problema no *link*, a TREVISO tem um link de contingência que entrará imediatamente em funcionamento.

Retorno ao ambiente de produção:

A equipe de TI-Infra informará aos usuários que o serviço retornou e/ou que o *link* foi restabelecido.

14.2.2. - Falha nos Servidores de *Firewall*

a) Abrangência:

Abriga o *software* de segurança.

b) Contingências existentes:

- 2 equipamentos configurados com alta disponibilidade em *Cluster* e ativação automática em caso de falhas;

- Empresa externa tem acesso remoto para casos de contingência.
- Tempo estimado 1h

Caberá à Gerência de Tecnologia e Segurança da Informação – INFRA/APOIO, comunicar a ocorrência ao órgão regulamentador Bacen.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Retorno ao ambiente de produção em caso de falha de *hardware* e/ou *software*:

Após o fechamento dos sistemas, a equipe fará os procedimentos inversos, realizando todos os testes necessários no ambiente de produção.

14.2.3. - Falha no Banco de Dados SQL

a) Abrangência:

O Banco de Dados SQL abriga as bases de sistemas corporativos e cadastro de clientes.

b) *Contingências existentes:*

- Servidor de contingência com replicação on-line (Cloud);
- Backup em rede, dados do dia anterior;
- Tempo estimado 2h

Caberá à Gerência de Tecnologia e Segurança da Informação – INFRA/APOIO, comunicar a ocorrência ao órgão regulamentador Bacen.

IMPORTANTE: A “RTM” fornece seus Serviços com disponibilidade anual de 99,3%, não devendo a duração da falha individual ser superior a 240 (duzentos e quarenta) minutos, incluindo deslocamento, diagnóstico, solução e normalização. O MTBF deverá ser igual ou superior a 30 (trinta) dias e o MTTR não superior a 120 (cento e vinte) minutos, sendo ambos apurados em períodos anuais.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Ativação da contingência em caso de falha de *hardware e/ou software*:

A área de TI-INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço. Caso não seja possível a disponibilização do serviço, serão acionados os seguintes procedimentos:

1. A área de TI-INFRA redirecionará os acessos para o servidor de contingência (Prazo estipulado 20min);

2. Depois de concluída a ativação da contingência, a área de TI-INFRA informará aos usuários, devendo estes se conectarem novamente à instância do banco de dados por meio dos sistemas, dando continuidade às tarefas do ponto onde haviam sido interrompidas. Durante o período em que o servidor de contingência estiver operando como produção, as rotinas de *backup* automatizadas serão alteradas para aquele servidor de contingência.

3. Comunicar a ocorrência ao *escalation* interno e ao órgão regulamentador BACEN.

Retorno ao ambiente de produção em caso de falha de *hardware e/ou software*:

O retorno, do ambiente de contingência para a produção, deverá ocorrer na noite da data subsequente em que este ambiente se encontrar disponível, após realizado o *backup* do banco de dados da contingência e replicação manual deste, para o ambiente de produção. O procedimento de retorno será disparado manualmente, através da execução de *scripts* de recuperação e ativação da produção. Depois de restabelecido o ambiente de produção, serão reativados os processos de replicação e *standby*, restabelecendo-se, assim, o ambiente de contingência e as rotinas de *backup* as quais serão alteradas, novamente, para o servidor de produção restabelecido.

14.2.4. - Falha na Rede - *Switch*

a) Abrangência:

*Switch*es

b) *Contingências existentes:*

A estrutura atual conta com uma contingência de barramento duplo, onde cada *switch* possui dois caminhos distintos para o *switch* de borda (principal). Em caso de queda de uma das conexões, a segunda entra em atividade automaticamente, evitando assim a perda de pacotes.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Ativação da contingência em caso de falha de *hardware* e/ou *software*:

A equipe de TI será notificada via *Total Network Monitor* e verificará o motivo da falha, adotando as medidas necessárias para a correção que, a depender do problema ocorrido, será:

- Problemas físicos na conexão - verificar se existe mal contato e/ou refazer o cabo, se necessário;
- Problemas físicos na porta do *switch* – desativar a porta danificada e substituir o ponto físico para outra porta livre. Após esse procedimento, providenciar a manutenção do equipamento em danificado junto ao fabricante;
- Problemas físicos no equipamento – remanejamento dos pontos para portas livres nos outros *switches*.

Retorno ao ambiente de produção:

A equipe de TI-INFRA retornará com o equipamento após a manutenção, restabelecendo todas as conexões após o fechamento dos sistemas. Tempo Previsto 3h

Comunicar a ocorrência ao órgão regulamentador, BACEN.

14.2.5. - Falha no Servidor de Arquivos

a) Abrangência:

O Servidor de arquivos abrange todos os diretórios da rede (ex: documentos de trabalho em MS Office, etc.), além de sistemas de terceiros e os programas-fonte do legado SIN.

b) *Contingências existentes:*

Backup em disco, dados do dia anterior.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Ativação da contingência em caso de falha de *hardware*:

A área de TI INFRA será acionada imediatamente, avaliando a extensão da falha e o prazo de retorno do serviço. (Prazo estimado 2h).

Comunicar a ocorrência ao órgão regulamentador, BACEN.

Retorno ao ambiente de produção em caso de falha de *hardware*:

O retorno do ambiente de contingência para o ambiente de produção ocorrerá na noite subsequente da data em que este ambiente estiver disponível.

14.2.6. - Falha no Sistema de Refrigeração da Sala dos Servidores

a) Abrangência:

A sala dos servidores abrange todos os servidores e serviços de Telecom.

b) *Contingências existentes:*

Dois equipamentos de ar condicionado que ficam ligados 24 horas.

c) Procedimentos:

Responsável: Gerência de Tecnologia e Segurança da Informação - INFRA/APOIO

Ativação da contingência em caso de falha de *hardware* e/ou *software*:

O segundo equipamento de ar permanecerá ligado, devendo a equipe de TI-INFRA providenciar a manutenção do equipamento principal, abrindo um chamado junto ao prestador de serviços especializados (HK Reformas Inst. e Manut de Equip. Eletro), especificamente contratado para proceder a manutenção e a prevenção, visando a solução do problema.

Retorno ao ambiente de produção:

A equipe de TI-INFRA ativará o equipamento danificado tão pronto este for restaurado.

15 – SEGURANÇA / BACKUP

Todo incidente e/ou problema, dúvidas ou demanda por suporte em tecnologia devem ser comunicados e/ou endereçados ao Departamento de Tecnologia e Segurança da Informação por meio de chamado técnico. Os colaboradores são orientados e instruídos a enviar e-mail para: suporte@trevisocc.com.br gerando, automaticamente, um "ticket" numerado que, a cada ação tomada, informa o requisitante sobre quanto à situação de tratamento do chamado e, dessa forma, permite quantificar, avaliar impacto e melhorar a gestão a partir dos fatos ocorridos, mitigando-se a possibilidade dos mesmos incidentes voltarem a ocorrer com objetiva minimização dos impactos e, garantia do fluxo produtivo.

A atualização das versões dos sistemas em uso segue as boas práticas do GMUD, as quais são testadas, pelo usuário, em ambiente de homologação e, somente após validado com sucesso e "aprovação" formalizada pelo usuário, ser aplicada em ambiente produção. Por medida de segurança, as versões atualizadas dos sistemas em uso, são disponibilizadas em ambiente de produção, sempre, após encerrado o expediente do último dia útil da semana (geralmente; sexta-feira), possibilitando, assim, tempo hábil para aplicar eventual plano de ação e impedir danos com impacto na produção diária.

Os serviços prestados pela "RTM" é composto pelas atividades de Monitoramento, Gerenciamento de Problemas, Gerenciamento de Desempenho e Gerenciamento de Configurações.

O monitoramento e gerenciamento dos serviços contratados pela Treviso é realizado de maneira preventiva, durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A "RTM" disponibilizará um Centro de Atendimento Especializado – NOC (*Network Operation Center*), que poderá ser acessado através de número de discagem gratuita, nos mesmos moldes de disponibilidade do gerenciamento dos serviços, com o objetivo de atender aos chamados originados pela Treviso, na prestação dos serviços descrito no objeto do contrato que rege a relação entre a parte contratante (Treviso) e a parte contratada ("RTM").

Se o problema não for resolvido em até 2 (duas) horas, a Treviso (contratante) poderá acionar a Liderança do NOC.

Se o problema não for resolvido em até 4 (quatro) horas, a Treviso (contratante) poderá acionar a Coordenação do NOC.

e

Se o problema não for solucionado em até 6 (seis) horas, a RTM mobilizará sua Diretoria de Operações (DIROP).

A atividade de Gerenciamento de Problemas consiste no monitoramento e detecção de eventuais falhas e visa, de forma proativa, solucioná-las.

A atividade de Gerenciamento de Desempenho consiste na coleta, processamento e disponibilização das informações sobre aspectos de desempenho dos serviços contratados.

A atividade de Gerenciamento de Configurações consiste na detecção e informação da configuração dos equipamentos de rede da Treviso (contratante), assim como no controle e configuração desses elementos.

O controle da configuração dos equipamentos de rede pressupõe a autorização da Treviso (contratante) à "RTM" para reconfigurar cada equipamento sempre que houver alteração na topologia lógica ou física da rede, ou quando a mesma for afetada por alguma falha.

São utilizados os mecanismos mais efetivos para combater possíveis tentativas de acessos indevidos, dentre eles:

- Security Operation Center – monitoramento;
- Estrutura de Firewall;
- IPS - Intrusion Prevention System;
- Proteção com antivírus, anti-malware;
- Redes segmentadas para garantir a segurança e a confidencialidade dos dados.

Os serviços de backup têm como objetivo guardar cópias de segurança dos dados do usuário, armazenados nas máquinas localizadas na "RTM".

A "RTM" fará toda a operação e administração do backup das informações do cliente em equipamentos próprios, permitindo:

a) Restauração em eventuais perdas dos dados de forma acidental pelos usuários; e

b) Recuperação dos dados em qualquer episódio de problemas lógicos nos sistemas físicos nos hardwares, ou até provenientes de catástrofes naturais nos ambientes da RTM em que as máquinas servidoras estão hospedadas. Essa recuperação inclui incidentes provocados pelas máquinas dos clientes da Treviso (contratante), desde que os dados sejam processados pelas máquinas servidoras localizadas na "RTM", e estejam incluídas nas rotinas de backup.

Todos os *backups* (local e nuvem) devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup (local e nuvem) deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, dentre outros.

As mídias de backup (configurando a fitoteca da RTM composta por mídias tais como; DAT, DLT, LTO, DVD, CD) são acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter (físico).

As fitas de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão orçamentária que assegure a renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup, rotina sob a incumbência da Gerência de Tecnologia da Informação.

Os *backups* imprescindíveis, críticos, para o bom funcionamento dos negócios do Treviso, em linha com as definições contidas no PCN da Treviso, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a classificação da Informação (SQL, Diretório Físico, etc.), seguindo assim as determinações fiscais e legais recomendadas e praticadas no país.

Na situação de erro de *backup* e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema, assegurando, dessa maneira, a continuidade da operação da Treviso.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados mediante justificativa de necessidade a ser apresentada via relatório, pela Gerência de Tecnologia da Informação, endereçado à Superintendência Administrativa.

Qualquer atraso na execução de *backup* ou *restore* deverão ser justificados formalmente, via relatório, endereçado à Superintendência Administrativa, pelos responsáveis da Gerência de Tecnologia da Informação.

Testes de restauração (*restore*) de *backup* são executados pela Gerência de Tecnologia e Segurança da Informação a cada 30 ou 60 dias, de acordo com a criticidade do *backup*.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e *restores*, a Gerência de Tecnologia da Informação preencherá formulário específico, passivo de ser auditado, interna e externamente.

Os colaboradores responsáveis pela restauração (*restore*) poderão delegar essa atividade a um terceiro especialmente contratado para realizar essa tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante (Gerência de Tecnologia e Segurança da Informação) não poderá se eximir da responsabilidade inerente à esse processo.

16 – DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança da informação, também, deve ser entendida como parte fundamental da cultura interna da Treviso, ou seja, qualquer incidente de segurança será considerado e tratado como se fosse e, como de fato é, um agente atuando contra a ética e os bons costumes regidos pela instituição no intuito de mitigar riscos e evitar possíveis incidentes.

Em casos de dúvidas ou esclarecimentos sobre o conteúdo desta Política, ou sobre a aplicação do mesmo em relação a algum assunto específico, o colaborador da TREVISO deverá entrar em contato a qualquer momento com a Gerência de Tecnologia da Informação.

A adesão à esta Política é obrigatória para todos os colaboradores da TREVISO e, ela ficará disponível para consulta, a qualquer tempo, na Intranet. Sua via física (impressa) será arquivada e estará disponível para consulta na Área de Compliance.

Cada funcionário assinará um Termo de Ciência e Responsabilidade, externando que tomou conhecimento da presente Política. O Termo de Ciência e Responsabilidade deverá ser formalizado (assinado) à cada atualização desta Política.

Este documento é de uso exclusivo da Treviso e, eventual pedido de compartilhamento com terceiros deverá ser submetido à Área de Compliance para ciência, análise e aprovação, devendo ser disponibilizado, exclusivamente, em meio físico (impresso) ou em documento digitalizado e protegido.

São Paulo, 22 de abril de 2021

Aprovado por:

A Diretoria
Treviso Corretora de Câmbio S/A.