Política de Segurança da Informação

Confidencialidade, Disponibilidade e Integridade

Área de Gestão de Compliance

Versão 2.2

I – Controle de Versão

Versão	Data	Nome	Ação (Elaboração, Revisão, Alteração)	Conteúdo
1.0	06/2016	Marcelo Couto	Elaboração	Elaboração do documento.
2.0	01/10/2017	Claudio Fernandes	Revisão	Revisão anual
2.1	01/11/2017	Claudio Fernandes	Alteração	Incorporação das discussões da reunião da Diretoria da Tercon
2.2	09/11/2017	Claudio Fernandes	Alteração	Incorporação das discussões da reunião da Diretoria da Tercon
	13/11/2017	Diretoria Tercon	Aprovação	

II – Sumário Executivo

Objetivos da Política:

- Assegurar o controle de informações confidenciais a que tenham acesso os colaboradores da **Tercon** (IN 558, art. 21, I);
- Assegurar a existência de testes periódicos de segurança para sistemas de informações (IN 558, art. 21, II);
- Proteger os clientes, a imagem da **Tercon** e as informações pertencentes a ambos;
- Garantir a continuidade do negócio de forma que não haja interrupção dos serviços prestados aos clientes da **Tercon**;
- Reduzir os riscos de fraudes, espionagens, sabotagem, vandalismo, problemas causados por vírus, erros, uso indevido e roubo de informações e diversos outros problemas que possam comprometer os princípios básicos da segurança da informação; e
- Definir as regras aplicáveis com base na estrutura da **Tercon**.

Áreas de Atuação nos termos da IN (Instrução Normativa) 558 da CVM:

Área	Atua
Gestão de carteiras	Sim
Consultor de Valores Mobiliários	NÃO
Distribuição dos Fundos próprios	Sim
Administração Fiduciária	NÃO

Produtos:

- Fundos de Investimento Multimercado (FIM);
- Fundo de Investimento em Direito Creditório (FIDC);
- Fundo de Investimento em Participações (FIP); e
- Fundo de Investimento Imobiliário.

Diretores Responsáveis:

Gestão	Luiz Fernando Conte Vasconcellos	Riscos	Marcelo Alberto Couto
Distribuição	Luiz Fernando Conte Vasconcellos	Compliance	Marcelo Alberto Couto
Suitability	Luiz Fernando Conte Vasconcellos	PLDFT	Marcelo Alberto Couto

III – Introdução

Informação compreende qualquer conteúdo ou dado que tenha valor para uma determinada empresa ou pessoa e que possa ser armazenado, transferido ou manipulada de algum modo, servindo a determinado propósito (e.g., tomada de decisão). Ela pode estar guardada para uso restrito ou exposta ao público para consulta ou aquisição.

Dentro deste contexto, toda e qualquer informação deve ser correta, precisa e estar disponível para a pessoa adequada. Portanto, Segurança da Informação[1] se refere à proteção existente sobre as informações de uma determinada empresa ou pessoa.

Uma política de segurança[2] consiste num conjunto formal de regras que devem ser seguidas pelos usuários de informações de uma organização ou de uma pessoa.

IV – Princípios Básicos da Segurança da Informação

- **Confidencialidade**: limita o acesso a informação tão somente às pessoas ou instituições autorizadas pelo proprietário da informação;
- **Integridade**: garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição),
- **Disponibilidade**: garante que a informação esteja sempre disponível para o uso por aqueles usuários autorizados pelo proprietário da informação.

V – Confidencialidade (IN 558, art. 25, II)

V.1 – Informações Confidenciais

São consideradas informações confidenciais para a **Tercon** todo tipo de informação escrita, verbal ou apresentada de modo tangível ou intangível acessadas pelo colaborador em virtude do desempenho de suas atividades que possa incluir:

- Know-how, técnicas, diagramas, modelos e programas de computador;
- Informações técnicas, financeiras, mercadológicas ou relacionadas a estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e fundos de investimento geridos pela **Tercon**;

[1] O conceito de Segurança da Informação está padronizado pela norma ISO/IEC 17799:2005, influenciada pelo padrão inglês (British Standard) BS 7799.

[2] RFC 2196 (The Site Security Handbook)

- Operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para os fundos de investimento geridos pela **Tercon**;
- Estruturas e planos de ação;
- Relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços;
- Qualquer informação relativa às atividades da **Tercon** e a seus sócios ou clientes;
- Informações e recursos disponíveis a projetos e trabalhos críticos para a continuidade do negócio da organização; e
- Toda e qualquer informação que por força de lei seja obrigatório o sigilo e confidencialidade.

V.2 – Informações de Uso Público

São consideradas informações de uso público todas as informações que por força de lei a **Tercon** é obrigada a divulgar à CVM e/ou para qualquer entidade de classe que a **Tercon** faça parte, desde que não conflite com o item V.1.

V.3 – Avisos Importantes em E-mails

Todos os e-mails da **Tercon** que possuem informações confidenciais devem conter *disclaimer* nos seguintes termos:

Esta mensagem pode conter informação confidencial e/ou privilegiada. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não pode usar, copiar ou divulgar as informações nela contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu esta mensagem por engano, por favor avise imediatamente o remetente, respondendo o e-mail e em seguida apague-o.	This message may contain confidential and/or privileged information. If you are not the addressee or authorized to receive this for the addressee, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by reply e-mail and delete this message.

V.4 – Avisos importantes em apresentações

Toda apresentação a clientes, contrapartes comerciais, fornecedores e prestadores de serviços que contenham informações classificadas como confidenciais deve conter:

- Aviso que o material é confidencial e de propriedade da **Tercon** e
- Todas as páginas devem conter a mensagem de “informação confidencial”.

V.5 – Transporte de Informações Confidenciais

É terminantemente proibido aos Colaboradores fazer cópia (física ou eletrônica) de arquivos contendo informações confidenciais ou não de propriedade da **Tercon** e circular em ambientes externos a empresa com estes arquivos sem a devida autorização da Diretoria da **Tercon**.

V.6 – Segregação de Atividades

A administração de carteiras de valores mobiliários deve ser segregada das demais atividades exercidas pela pessoa jurídica, por meio da adoção dos seguintes procedimentos (IN 558, art. 24).

V.6.1. Segregação entre Administração de Carteiras e Área de Distribuição

Nos termos do parágrafo único do art. 24 da IN 558, a área de administração de carteiras não precisa ser segregada fisicamente da área de distribuição tendo em vista que a **Tercon** somente distribui fundos de investimentos sob sua gestão.

V.6.2. Segregação entre Gestão e Risco/Compliance

A **Tercon** não adota a segregação física entre gestão e as áreas **independentes** de risco e compliance. A Tercon entende que o monitoramento do cumprimento aos princípios éticos e as normas legais deve ser feito, coordenada e executada de forma continua e a atuação para a correção de qualquer desvio deve ser feito tempestivamente, buscando a educação e o comprometimento dos colaboradores na adoção de boas práticas de mercado e seguir o código de ética da Tercon.

Com isso, essa forma de trabalho requer que Compliance e Risco não fiquem isolados em uma sala.

V.6.3. Criação e Manutenção de Usuários

Com a finalidade de preservar informações confidenciais e permitir a identificação das pessoas que tenham acesso a elas (IN 558, art. 24, II), os acessos internos e externos aos serviços de rede da **Tercon** são liberados de acordo com a função que o Colaborador exerce na empresa e de acordo com a sua necessidade. O Diretor da Área é o responsável por definir os acessos dos seus respectivos Colaboradores.

O acesso externo é concedido em caráter de exceção somente com a autorização da diretoria Tercon, tendo este que ser justificado e montada toda uma infraestrutura de monitoramento e segurança para assegurar o controle de acesso e a segurança das informações confidenciais.

Quando do desligamento de Colaboradores, o seu acesso à rede e e-mail é revogado a partir do momento que o desligamento for informado à Área de TI.

V.6.4. Proteção de Senhas

De forma a alcançar os mesmos objetivos do item anterior, a criação de acesso dos usuários descritos no item anterior requer a criação de senha de acesso pessoal para cada usuário. Além disso, os Colaboradores devem ter ciência de que a senha e *login* para acesso aos dados contidos em todos os computadores, inclusive nos e-mails, são pessoais, comprometendo-se a mantê-los em sigilo e não os divulgar para quaisquer terceiros

V.7 – Firewall

A alteração da configuração do firewall é feita somente pela área de TI.

O monitoramento do firewall é realizado pela área de TI.

VI – Integridade

Para garantir a integridade das informações, a **Tercon** adota os seguintes procedimentos para reduzir o ataque de ameaças externas que possam corromper as informações arquivadas:

VI.1 – Correio Eletrônico

O e-mail da **Tercon** é de uso estritamente profissional, não devendo ser utilizado para fins pessoais. Os Colaboradores não poderão usar intencionalmente o e-mail da **Tercon** para distribuir "correntes", brincadeiras, enviar material ofensivo, inadequado, vírus ou que promova qualquer tipo de discriminação racial. Se o Colaborador receber um e-mail para distribuição a outras pessoas, como uma corrente, não poderá enviá-lo. Se tiver qualquer suspeita de que recebeu um vírus, o Colaborador deverá entrar em contato com a Área de TI imediatamente.

VI.2 – Internet

A internet da **Tercon** é de uso estritamente profissional, não devendo ser utilizada para fins pessoais. Os Colaboradores não poderão entrar em sites com conteúdo ofensivo, inadequado ou que promova qualquer tipo de discriminação racial, social ou moral.

Monitoramento: a área administrativa poderá monitorar os sites que os Colaboradores navegam de forma a verificar se estes estão utilizando a Internet somente para fins profissionais.

VI.3 – Instalação e Download de Softwares

Todo software somente poderá ser instalado mediante autorização prévia da Área de TI.

Caso seja necessário fazer algum download, o Colaborador deverá solicitar autorização prévia junto a Área de TI.

Download de aplicativos: é proibido baixar qualquer tipo de software não autorizado pela Diretoria em função de aplicativos não autorizados poderem abrir brechas no firewall da Tercon.

VI.4 – Proteção Antivírus

O servidor e os computadores da **Tercon** utilizam antivírus cuja atualização é realizada todos os dias de forma automática.

O antivírus está configurado de forma a verificar ameaças da internet, de e-mails e de toda e qualquer origem de fonte de informação externa a organização.

A renovação da licença do antivírus é realizada automaticamente.

VI.5 – Monitoramento dos Meios de Comunicação

O intermediário que atue em mercado organizado deverá manter sistema de gravação de todos os diálogos e mensagens mantidos com seus clientes, inclusive por intermédio de prepostos, de forma a registrar as ordens transmitidas por telefone ou outros sistemas de transmissão de voz.

Para as demais situações, a Tercon realiza as operações aprovando-as pelo sistema do custodiante, o qual possui trilha de auditoria. Além disso, ela não fecha nenhuma operação por telefone. Todas as condições negociais só são concretizadas via formalização contratual.

Para assegurar o fiel cumprimento das regras internas, como também da legislação vigente, a Tercon se reserva no direito de rastrear, monitorar, gravar e inspecionar todos e qualquer tráfego de voz realizado através de contato telefônico e internet, bem como troca de informações escritas transmitidas via: internet, intranet, sistema de mensagem instantânea, fax, correio físico e eletrônico (e-mail), bem como os arquivos armazenados ou criados pelos recursos da informática pertencentes a Tercon ou utilizados em nome dela.

VI.6 – Monitoramento da Rede

A área de TI é responsável pelo monitoramento da rede. Ela verifica continuamente a integridade desta e controla tentativas de invasão.

VI.7 – Monitoramento dos Sistemas

- Execução de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico.

- Execução de auditorias e inspeções nos registros e verificação se os sistemas são protegidos contra adulterações.

VII – Disponibilidade

VII.1 – Segurança dos Processos Vitais

Entende-se por ativos vitais todos aqueles que, em caso de roubo, explosão, incêndio, quebra, perda ou mau funcionamento, podem prejudicar o andamento do processo de seleção e alocação de ativos da **Tercon** e trazer perdas para a mesma e/ou aos seus clientes.

Os equipamentos e serviços vitais da **Tercon** estão descritos no Plano de Continuidade de Negócios.

Quando ocorrer impossibilidade de acesso aos equipamentos e serviços vitais, a contingência deverá ser acionada de acordo com o Plano de Continuidade de Negócios.

A área de Compliance deve avaliar quais equipamentos vitais devem possuir seguro contra roubo, furto, incêndio e explosão. A responsabilidade pela contratação e renovação do seguro é de responsabilidade do Diretor de Financeiro.

Vide Plano de Continuidade de Negócios.

VII.2 – Manutenção de Arquivos

Todo e qualquer arquivo, documento, relatório, pesquisa, banco de dados, sistema e planilha da **Tercon** deverá ser salvo na rede.

A **Tercon** deve manter digitalmente, pelo prazo mínimo de 5 (cinco) anos, ou por prazo superior por determinação expressa da CVM, todos os documentos e informações exigidos pela CVM, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções (IN 558, art. 31).

É de responsabilidade de todos os Colaboradores gravar e manter as informações da **Tercon** na rede.

VII.3 – Plano de Continuidade dos Negócios

O Plano de Continuidade dos Negócios consiste de um conjunto de planos de ação de maneira a garantir que os serviços vitais sejam devidamente identificados e preservados após a ocorrência de qualquer situação que afete os processos críticos do negócio e até o retorno à situação normal de funcionamento da **Tercon**.

Vide Plano de Continuidade dos Negócios para consultar detalhes.

VII.4 – Monitoramento

Para garantir a continuidade dos serviços, os recursos dos equipamentos devem ser constantemente monitorados, permitindo não só a identificação de possíveis problemas, mas também futuras atualizações de acordo com a tendência de crescimento de seus programas e aplicativos.

O monitoramento desses recursos deve verificar: espaço disponível em disco, processamento, utilização de memória, inventário de segurança, conectividade, estabilizadores e conectividade de rede.

VII.5 – Realização de Cópias de Segurança

Cópias de segurança dos dados do servidor e da nuvem são feitas diariamente. Há redundância dos servidores (um local e outro em sítio remoto).

VII.6 – Testes de Atendimento a Esta Política (IN 558, art. 21, II)

A área de compliance é responsável pela execução de testes para certificar que todos os procedimentos aqui descritos foram implementados e estão sendo seguidos por todos os Colaborares.

A execução dos testes é anual e as evidências devem ser armazenadas pelo período de 5 (cinco) anos.

VIII – Adesão à Política de Segurança da Informação

Para garantir os princípios da segurança da informação, é preciso assegurar que cada Colaborador esteja em conformidade com as normas descritas nessa Política e nas leis que regem o setor de atuação da **Tercon**. Além disso, a gestão da segurança da informação necessita do apoio e participação de todos os Colaboradores.

Para tanto, são necessários os três passos a seguir:

- Treinamento e compreensão a essa política (IN 558, art. 21, III);
- Assinatura do Termo de Compromisso e Confidencialidade (Anexo I do Código de Ética); e
- Reciclagem anual.

O cumprimento desses três passos é de responsabilidade do Diretor de Risco e Compliance, o qual seguirá as seguintes regras:

- Processo de integração e treinamento inicial dos Colaboradores, aos quais, antes do início de suas atividades, será apresentada a Política de Segurança da Informação em conjunto com o Plano de Continuidade de Negócios da **Tercon**, bem como as principais leis e normas aplicáveis às suas atividades;
- Toda e qualquer dúvida, questionamento, sugestão ou pedido de esclarecimento relacionado a tal Política e a tal Plano, ou quaisquer outras, deverão ser respondidos em até 3 (três) dias úteis para que os Colaboradores possam compreendê-los e observá-los integralmente no desempenho das suas respectivas atividades; e
- O programa anual de reciclagem dos Colaboradores tem a sua participação obrigatória, com o objetivo de fazer com que os mesmos estejam sempre atualizados em relação às regras de segurança da informação aplicáveis pela **Tercon**.