Política de Segurança da Informação e Cibersegurança

Índice

1. OBJETIVO E ABRANGÊNCIA

1.1. Esta Política de Segurança da Informação e Cibersegurança ("Política de Cibersegurança") tem por objetivo estabelecer diretrizes e procedimentos de cibersegurança e segurança da informação a serem observados pela Estar S.A., na qualidade de administradora de mercado de balcão organizado ("Sociedade"), buscando garantir que os recursos computacionais e a manipulação de dados estejam de acordo com o nível de segurança exigido pela Sociedade e pelos órgãos reguladores, bem como nortear a definição de normas e procedimentos específicos de segurança da informação, tal qual a implementação de controles e processos para seu atendimento, visando proteger a Sociedade, os Investidores, Emissores e o público em geral, observado o disposto no Regulamento do Mercado de Balcão Organizado da Estar ("Regulamento").

1.2. A informação é um dos principais geradores de valor para uma instituição e a qualidade do fluxo de dados é o principal subsídio para tomada de decisão e interpretação dos movimentos do negócio. Como consequência, é importante um acompanhamento constante no intuito de combater riscos e ameaças, ao mesmo tempo em que se atue de maneira a manter a integridade e segurança dos dados (sejam eles *online* ou *offline*).

1.3. Esta Política de Cibersegurança aplica-se aos administradores, colaboradores, pessoas naturais ou jurídicas que sejam, direta ou indiretamente, controladoras ou participem do controle societário da Sociedade, bem como terceiros que tenham relação comercial, profissional ou de confiança com a Sociedade, incluindo, sem limitação, membros externos, empresas controladas, coligadas ou do mesmo grupo econômico da Sociedade, prestadores de serviços, funcionários e estagiários de empresas controladas, coligadas ou do mesmo grupo econômico da Sociedade e quaisquer pessoas que tiverem relação com a Sociedade, ainda que com nomes, responsabilidades ou funções diversas das supracitadas, que de alguma forma tenham cargo, função ou posição de natureza trabalhista, comercial, societária ou quaisquer outras que permitam o acesso à informações do Grupo Estar, dos Investidores e dos Emissores ("Pessoas Sujeitas")

1.4. Palavras e expressões iniciadas em letra maiúscula, em suas formas no singular e no plural, e de outra forma não definidos nesta Política de Cibersegurança, terão os significados a eles atribuídos no Glossário Estar, disponível no website da Sociedade.

2. CONCEITOS

2.1. A segurança da informação aqui é caracterizada pela preservação dos seguintes conceitos:

(i) **Confidencialidade:** garantia de que a informação e dados somente possam ser acessados por pessoas autorizadas, pelo período necessário;

(ii) **Disponibilidade**: garantia de que a informação e os dados estejam disponíveis para as pessoas autorizadas quando se fizerem necessários; e

(iii) **Integridade**: garantia de que a informação esteja completa, exata, íntegra e que não tenha sido modificada ou destruída indevidamente, de maneira não autorizada ou acidental durante o seu ciclo de vida.

3. DEFINIÇÕES

(i) Software: é a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores, assim como o conjunto organizado de instruções em linguagem natural ou codificada, contida em suporte de qualquer natureza, de emprego necessário em máquinas automáticas de tratamento da informação, dispositivos ou instrumentos ou equipamentos periféricos, baseados em técnica digital ou análoga, para fazê-los funcionar de modo e para fins determinados. Toda interação dos usuários de computadores é realizada através de softwares.

(ii) Backup: é a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver falhas no sistema, como apagamentos acidentais ou corrupção de dados.

(iii) Mídias removíveis: dispositivos que permitem a leitura e gravação de dados, tais como: CD, DVD, Disquete, Pen Drive, cartão de memória, entre outros.

(iv) Virtual Private Network (VPN): modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios, como se o mesmo estivesse conectado física e diretamente à rede interna. Somente Investidores e/ou Emissores que detém Autorização e acesso ao VPN terão acesso interno a rede do Mercado Estar, com recursos limitados.

(v) Virtual Private Cloud (VPC): para maior segurança do Mercado Estar, as redes privadas do Mercado Estar e a Estar utilizam como provedor de serviços o VPC da Google Cloud, permitindo que a Estar controle aqueles que possuem acesso aos seus sistemas. Nenhum sistema externo terá acesso direto aos sistemas principais do Mercado Estar, sendo certo que tais acessos são realizados por um sistema *gateway* com ferramentas que viabilizam inibir ataques DDoS, invasão, bloqueio de IPs e limite de requisições.

(vi) Firewall: é um dispositivo de uma rede de computadores que tem por objetivo monitorar o tráfego de rede de entrada e saída, permitindo ou bloqueando tráfegos específicos, em conformidade com as regras de uma política de segurança a um determinado ponto da rede.

(vii) Informação da Sociedade: toda informação sobre a Sociedade, seus colaboradores, fornecedores, terceiros, clientes e diretores.

(viii) Responsável pela Informação: também conhecido como gestor de sistema e/ou de informação, é a pessoa responsável perante a Sociedade por classificar quaisquer informações, sendo elas da Sociedade ou geradas pelos seus respectivos profissionais, e os ativos associados aos recursos de processamento da informação e assegurar, que estejam protegidos quanto aos critérios da confidencialidade, integridade e disponibilidade durante todo seu ciclo de vida (geração, acesso, manuseio, armazenamento, reprodução, transporte e descarte).

4. DIRETRIZES

4.1. A informação processada em softwares constitui-se ativo valioso e de extrema importância para a Sociedade e fundamental para o sucesso de seus negócios, merecendo, portanto, proteção adequada.

4.2. Segurança de informação *online* ou *offline* consiste na adoção de medidas para proteger a propriedade, confidencialidade, disponibilidade e integridade da informação que circula na internet, em qualquer forma e suporte que se apresente, das diversas ameaças existentes, a fim de evitar seu uso indevido, inadequado, ilegal ou em desconformidade com as políticas e procedimentos internos da Sociedade. Para tanto, devem ser observadas as diretrizes a seguir indicadas.

A. Propriedade, monitoramento e classificação da informação

4.3. As informações produzidas pelas pessoas abrangidas por esta Política de Cibersegurança (em formato físico ou digital) são de propriedade exclusiva da Sociedade bem como as informações a ela disponibilizadas, de maneira autorizada, por terceiros, devendo ser utilizadas exclusivamente para o atendimento dos objetivos do negócio.

4.4. Os equipamentos, meios de comunicação e sistemas do Mercado Estar estão sujeitos a monitoramento pela Sociedade, sendo certo que eventuais informações de cunho pessoal tratadas por esses meios ou fornecidas à Sociedade serão abrangidas por referido controle, sendo tratadas nos termos da Política de Privacidade da Sociedade. O monitoramento aqui previsto é de conhecimento de todos os abrangidos por esta Política de Cibersegurança.

4.5. A Sociedade classifica as informações mencionadas nesta Política de Cibersegurança de acordo com o nível de confidencialidade e criticidade para o negócio da Sociedade, conforme caracterizadas na cláusula 6 abaixo, em:

(a) Informação pública;

(b) Informação pessoal;

(c) Informação pessoal sensível;

(d) Informação interna;

(e) Informação confidencial; e

(f) Informação restrita.

4.6. A classificação das informações será atribuída pelos responsáveis pela Informação, formalmente designados como responsáveis pela autorização de acesso às informações sob a sua responsabilidade, variando de acordo com o teor de cada informação.

4.7. As informações devem estar adequadamente protegidas e rotuladas em observância às diretrizes de segurança da informação cibernética da Sociedade em todo o ciclo de vida, que compreende: geração, acesso, manuseio, armazenamento, reprodução, transporte e descarte.

4.8. Toda informação – *online* ou *offlin*e – que seja propriedade da Sociedade deve ser protegida de qualquer ameaça que possa comprometer sua confidencialidade,

integridade ou disponibilidade, através de softwares específicos de segurança da informação e/ou de cibersegurança.

4.9. A Sociedade adota postura prospectiva no gerenciamento de cibersegurança e proteção de dados, atuando com procedimentos e controles que reduzam sua vulnerabilidade a falhas e incidentes. Deve ser considerado como incidente de segurança da informação todos os eventos não autorizados que tenham por finalidade burlar controles de segurança para comprometer a confidencialidade, integridade, disponibilidade ou privacidade de dados. Também devem ser considerados eventos acidentais ou ocasionados pelo descumprimento de controles. Todo incidente deve ser registrado e endereçado ao responsável pela atuação e solução. Obrigatoriamente, deve ser realizada análise de causa raiz e impacto de todos os incidentes para que planos de ação corretivos sejam implantados e o risco de reincidência mitigado. A gestão de incidentes deve ser conduzida por time especializado e dedicado a esta atividade, o qual deve assegurar a identificação, proteção, detecção, reposta e recuperação de incidentes.

4.10. Qualquer evento ou situação irregular que configure descumprimento à esta Política de Cibersegurança ou incidente crítico de segurança cibernética, que tenha impacto significativo sobre a operação normal do Mercado SU ou sobre os Participantes do Mercado Estar será imediatamente reportado à SMI e ao Conselho de Autorregulação.

4.10.1. A comunicação para a SMI e ao Conselho de Autorregulação deverá contar com **(a)** avaliação sobre os tipos e o número de participantes potencialmente afetados, se houver; **(b)** medidas já adotadas pela Sociedade, ou as que pretende adotar; **(c)** tempo consumido na solução do evento ou prazo esperado para que isso ocorra; e **(d)** qualquer outra informação considerada importante pela Sociedade. Adicionalmente, a Sociedade irá atualizar as informações prestadas à SMI até a solução do incidente.

4.10.2. A Sociedade irá elaborar e manter à disposição da SMI relatório final contendo **(a)** descrição do incidente e das medidas tomadas, informando o impacto gerado pelo incidente sobre a operação do Mercado Estar e os Participantes; **(b)** cópia das comunicações realizadas, se houver; **(c)** cópia dos relatórios internos de investigação produzidos pela entidade ou por terceiros sobre a análise do incidente e as conclusões dos exames efetuados; e aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, se for o caso.

4.11. Independente da forma como é gerada, tratada ou compartilhada, toda informação sob propriedade da Sociedade deve ser utilizada unicamente para finalidade com a qual foi autorizada, observado o disposto na cláusula 8.2 desta Política de Cibersegurança.

4.12. O controle sobre o acesso físico deve abranger *hardware* e ambiente, devendo, inclusive, ser implementado controle que assegure a devolução, quando aplicável, dos mesmos em situações de desligamento e término contratual.

4.13. Os controles devem abranger a movimentação de ativos de informação (*hardware*) nas dependências da Sociedade, sendo devidamente autorizadas, monitoradas e registradas. Deve ser garantido o controle total sobre o ativo, seu estado e localização, e mitigando riscos de fraude, desvio e roubo.

B. Acesso e identidades

4.14. Os acessos às informações e aos ambientes tecnológicos da Sociedade devem ser controlados de acordo com sua classificação e revisados periodicamente pelo Diretor-Geral ou por área específica da Sociedade por este designada, de forma a serem disponibilizados apenas às pessoas autorizadas e com os privilégios necessários para o desempenho de suas atividades, observado o disposto na cláusula 8.2 desta Política de Cibersegurança.

4.15. No que tange à cibersegurança e proteção de dados, a Sociedade deve empregar esforços compatíveis com a natureza das suas operações e complexidade de seus produtos, bem como disseminar cultura de cibersegurança e proteção de dados a todos os seus colaboradores, desde a fase de concepção de um produto ou de um serviço até a sua execução.

C. Descarte de dados

4.16. O descarte de dados deve ser realizado com o emprego de medidas que impossibilitem a sua reconstrução, de acordo com as necessidades do suporte digital. Os dados devem ser descartados considerando prazos mínimos legais ou regulatórios, bem como sua necessidade para o negócio ou a área e a finalidade pela qual foram inicialmente coletados o que for maior.

4.17 Deverá ser considerada a natureza das informações, assim como a finalidade do tratamento da informação, uma vez que a tenha sido exaurida, as informações deverão ser eliminadas.

4.18 Durante o descarte, a Sociedade deve assegurar que medidas técnicas, administrativas e legais apropriadas sejam aplicadas às informações para protegê-las contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícita.

O descarte deve ocorrer, preferencialmente, da seguinte forma:

a. Para informações em meio digital: para a destruição de documentos digitais, deve-se utilizar software e procedimentos homologados pela área de Segurança da Informação, e que, assegurem a impossibilidade de recuperação dos mesmos;

b. Para informações em meio físico: para a destruição de equipamentos, deve-se utilizar recursos e procedimentos específicos, homologados pela área de Segurança da Informação, e que, assegurem a impossibilidade de recuperação dos mesmos.

D. Fornecedores e Partes Externas

4.19. Os contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos dados, aos sistemas e/ou ao ambiente do Mercado Estar devem conter cláusulas que assegurem o cumprimento das regras de segurança cibernética, bem como penalidades no caso de descumprimento.

4.20. A contratação de serviços relevantes, fornecedores e terceiros que atuem no processo e armazenamento de dados deve obedecer, além do estipulado neste item, às disposições específicas na Cláusula 8 desta Política de Cibersegurança.

4.21. A Sociedade deve manter o controle sobre os riscos envolvidos na contratação e prestação de serviços, garantindo que controles sejam implementados e revisados periodicamente para a mitigação a um nível aceitável.

5. RESPONSABILIDADES

5.1. As Pessoas Sujeitas devem:

(i) cumprir as regras de segurança da informação e dados aqui previstas, na legislação aplicável e nas demais Políticas Estar;

(ii) proteger as informações e dados contra acessos, modificação, destruição ou divulgações não autorizadas, em especial quanto ao disposto no Capítulo III do Regulamento;

(iii) assegurar que os recursos tecnológicos, as informações, os dados e os sistemas a sua disposição sejam utilizados apenas para as finalidades da Sociedade;

(iv) cumprir as leis e as normas que regulamentam a propriedade intelectual;

(v) cumprir as leis e normas que regulamentem a privacidade e proteção de dados pessoais;

(vi) não discutir, citar ou compartilhar assuntos confidenciais em ambientes públicos ou em áreas expostas (aviões, transportes, restaurantes, encontros sociais, etc.), incluindo comentários e opiniões em blogs e redes sociais;

(vii) não compartilhar informações e dados confidenciais de qualquer tipo; e

(viii) comunicar imediatamente os responsáveis pela segurança de informações e dados qualquer descumprimento ou violação desta Política de Cibersegurança e/ou de suas normas e procedimentos.

5.2. É dever do Diretor-Geral:

(i) reforçar e orientar os Colaboradores da Sociedade em relações a práticas, processos de segurança e acessos a sistemas para o desempenho e eficácia da segurança;

(ii) assegurar que as responsabilidade e autoridades dos papéis relevantes para a segurança da informação sejam atribuídas e comunicados;

(iii) promover a ampla divulgação desta Política de Cibersegurança e das normas de segurança da informação e dados;

(iv) promover ações de conscientização sobre segurança da informação e dados para os colaboradores;

(v) propor ações de aperfeiçoamento da segurança da informação e dados;

(vi) estabelecer normas e procedimentos relacionados à instrumentação da segurança da informação e dados, dispondo sobre a propriedade e o uso da informação e dos dados, a gestão de acessos e identidades e os incidentes de segurança das informações e dos dados;

(vii) a cada 12 (doze) meses, realizar análise dos controles exarados na ISO/IEC 27002, conforme aplicáveis à Sociedade, a fim de garantir a melhoria contínua dos procedimentos de proteção;

(viii) realizar ou coordenar a realização de treinamentos, no mínimo anualmente, destinados a divulgar as regras, procedimentos e controles internos relacionados a confidencialidade, a integridade, incidentes de segurança da informação e a disponibilidade dos dados e informações sensíveis aos Colaboradores da Sociedade, em especial aqueles que tenham acesso a dados e informações sensíveis da Sociedade;

(ix) gestão de cibersegurança e proteção de dados, tendo como atuação a proposição de ajustes, melhorias, aprimoramentos, validações e modificações desta Política de Cibersegurança;

(x) executar todas as atividades para a gestão de segurança da informação;

(xi) realizar a gestão de controle, distribuição e instalação de softwares utilizados;

(xii) colaborar juntamente à unidade organizacional pela gestão de riscos e de capital para melhoria contínua da operação;

(xiii) mapear eventuais incidentes de vazamento de informações e incidentes de probabilidade significativa;

(xiv) estabelecer procedimento de resposta à incidentes que envolvem dados pessoais à ANPD, quando aplicável;

(xv) coordenar a realização dos testes periódicos de avaliação da vulnerabilidade da Sociedade contra ataques cibernéticos;

(xvi) estabelecer formas de participação em iniciativas que objetivem o compartilhamento de informações sobre ameaças e vulnerabilidades relevantes;

(xvii) elaborar relatório anual que conste os incidentes registrados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da cibersegurança; e

(xviii) mediante envio de Ofício, comunicar aos Membros do Mercado Estar a respeito de questões relacionadas à segurança da informação, cibersegurança e indícios de incidentes de violação das informações do Mercado Estar, caso aplicável.

5.3. Áreas internas da Sociedade: assegurar que contratos com as empresas prestadoras de serviços que possuem acesso às informações, aos dados, aos sistemas e/ou ao ambiente do Mercado Estar e da Sociedade contenham cláusulas que assegurem o cumprimento das regras de segurança cibernética, bem como penalidades no caso de descumprimento.

6. DA CLASSIFICAÇÃO DA INFORMAÇÃO E DOS DADOS

6.1. Todas as informações sob a responsabilidade da Sociedade devem ser classificadas e protegidas conforme seu grau de confidencialidade e privacidade, devendo ser estabelecidos processos, controles, papéis e responsabilidades que assegurem a devida classificação e proteção durante todo o seu ciclo de vida. As informações e os dados, nos termos desta Política de Cibersegurança, são classificados em:

(i) **Pública**: toda informação e dados de propriedade da Sociedade oriunda de base pública e/ou com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou proporcional, sendo destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma;

(ii) **Pessoal**: toda informação relacionada a pessoa natural identificada ou identificável;

(iii) **Pessoal Sensível**: é toda informação sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter

religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

(iv) **Interna**: é toda informação de propriedade da Sociedade que esta não tem interesse em divulgar, onde o acesso por parte de indivíduos externos à empresa deve ser evitado, isto é, informações acerca dos negócios da Sociedade, estratégicas e de seu ambiente corporativo, não sendo relativas ao Mercado Estar. Caso esta informação seja acessada indevidamente, poderá causar danos mínimos ou irrelevantes à imagem do Mercado Estar, o que permite seu acesso sem restrições por todos os empregados e prestadores de serviços da Sociedade;

(v) **Confidencial:** é toda informação de propriedade da Sociedade considerada crítica para os negócios da Sociedade e para o Mercado Estar e cuja divulgação não autorizada pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais. É sempre restrita a um grupo específico de pessoas da Sociedade e, aos fornecedores ou prestadores de serviços da Sociedade, excepcionalmente em casos específicos a serem analisados pelo Diretor-Geral, nos quais a informação seja relevante para o desenvolvimento de suas atividades;

(vi) **Restrita**: é toda informação de propriedade da Sociedade que pode ser acessada somente por usuários do Mercado Estar. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização ou do Mercado Estar.

7. MECANISMOS DE SEGURANÇA

7.1. Dentro dos procedimentos adotados para gerenciamento da Cibersegurança e proteção de dados, deve-se observar:

(i) **Segurança do ambiente físico**: Os servidores que armazenam os sistemas críticos à operação do Mercado Estar devem ser hospedados em Data Centers ou nuvem, que possuam acessos controlados e monitorados, bem como garantam disponibilidade dos ativos informacionais a Sociedade com perenidade, inclusive quando acionados os protocolos previstos no Plano de Continuidade de Negócios. Os Data Centers devem aderir às Políticas Estar bem como atender às quaisquer solicitações desta instituição, inclusive de

visitação, que deverá ser alinhada previamente com o respectivo provedor, além de garantir sua capacidade de resposta a incidentes e continuidade de negócio. Já as máquinas e estações de trabalhos dos colaboradores e terceiros que atuem na Sociedade devem ser protegidos contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Observa-se que estes ativos físicos devem utilizar apenas softwares licenciados ou autorizados pela unidade responsável, bem como é obrigatório o uso de software de Endpoint para fins de controle de ameaças eletrônicas, vírus, zero-day, ransonware.

(ii) **Segurança do ambiente lógico**: Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuadamente, com papéis de responsabilidade claramente definidos e registrados. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir os objetivos desta Política de Cibersegurança. Deve ser assegurado, no que se refere a acesso lógico, a identificação e o estabelecimento de segregação de função em atividades com potencial de conflito de interesse, em níveis operacionais, táticos e estratégicos. Deve haver um processo de revisão de acessos, que garanta a validação das permissões e da vigência de todos os acessos autorizados em ambiente lógico. Deve ser viabilizada a gestão das permissões e perfis de acesso, devendo garantir o direito ao privilégio mínimo de acesso, que visa conceder permissão apenas ao que é necessário para executar as atividades correspondentes a função do usuário, provendo condições para que as senhas de acesso sejam protegidas contra acesso não autorizado e, para acessos críticos, super usuários e administradores, a autenticação lógica aconteça sem que o usuário tenha conhecimento da mesma ou que contemple salvaguardada em dupla custódia, sempre que possível. Além disso, devem ser estabelecidos controles que restrinjam o acesso ao código fonte de sistemas e soluções tecnológicas da Sociedade, garantindo a preservação e integridade dos dados e dos recursos.

(iii) **Segurança do ambiente digital**:

(iv) **Autenticação e senha**: O usuário (seja colaborador, Investidor ou Emissor, conforme aplicável) é responsável por todos os atos executados com seu login e senha, sendo papel do usuário manter a confidencialidade de seus

dados e alterar a senha periodicamente, utilizando combinações de qualidade e difícil adivinhação. Também é papel do usuário bloquear seu equipamento sempre que se ausentar. Adicionalmente, recomenda-se que sejam estabelecidos controles que garantam o emprego: **(a)** de múltiplo fator de autenticação, sempre que possível; e **(b)** de criptografia em todo processo de autenticação e troca de informações assegurando a encriptação dos dados em trânsito.

(v) **Da mesa limpa e tela limpa**: O usuário deve adotar postura aderente as práticas relacionadas a assegurar que informações sensíveis, tanto em formato digital quanto físico, e ativos (e.g., notebooks, celulares, tablets, etc.) não sejam deixados desprotegidos em espaços de trabalho pessoais ou públicos quando não estão em uso. A Sociedade deve estabelecer controles que assegurem a conscientização e responsabilização de todos os colaboradores e terceiros quanto ao uso adequado de equipamentos e a proteção das informações durante todo o seu ciclo de vida.

(vi) **Do backup**: Os backups deverão ser realizados em nuvem e serem salvos em discos e/ou máquinas pré-configurados pelo provedor do backup. Os backups deverão ser executados de forma automática, diariamente, fora do horário comercial e podendo durar até 4 horas. Adicionalmente, os backups serão armazenados em diferentes regiões geográficas para a mitigação de desastres naturais e deverão ficar salvos pelo período de 1 (um) ano. Os backups podem ser utilizados para restauração total ou parcial do banco de dados.

(vii) **Da VPN**: O uso do acesso via VPN deve ser restrito e utilizado para as finalidades relacionadas com os negócios, devendo abster-se de usar a funcionalidade para quaisquer outras atividades, sendo vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

(viii) **Pentest** - Framework utilizado no Mercado Estar para a realização de teste de intrusão, visando encontrar potenciais vulnerabilidades em sistemas, servidores ou de forma geral em sua estrutura de rede.

(ix) **Da violação desta Política de Cibersegurança**: Nos casos em que houver violação desta Política de Cibersegurança, sanções autorregulatórias (nos termos do Regulamento) administrativas e/ou legais poderão ser adotadas,

sem prévio aviso, podendo culminar com o desligamento e eventuais processos administrativos, legais ou Processos Sancionadores, conforme aplicável.

(x) **Treinamentos periódicos**. Deverão ser realizados, no mínimo anualmente, treinamentos para os Colaboradores que devem contemplar explicações sobre as ameaças do setor da Sociedade, discussão de casos reais envolvendo incidentes de segurança da informação, ações a serem tomadas caso um Colaborador se depare com algum tipo de ameaça e realização de prova de entendimento do treinamento aplicado. Os treinamentos devem visar a explicação sobre os procedimentos e controles internos relacionados a confidencialidade, a integridade, incidentes de segurança da informação e a disponibilidade dos dados e informações sensíveis aos Colaboradores.

(xi) **Plano de Continuidade de Negócios**. Os Colaboradores devem observar a presente Política de Cibersegurança em conjunto com os procedimentos e mecanismos previstos no Plano de Continuidade de Negócio aprovado pelos administradores da Sociedade e o Conselho de Autorregulação.

8. CONTRATAÇÃO DE SERVIÇOS RELEVANTES, DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

8.1. A contratação de serviços relevantes para processamento e armazenamento de dados e de computação em nuvem são solicitadas através da unidade responsável pela Cibersegurança, que deve:

(i) observar a contratação com aderência à estratégia, apetite e gestão de riscos da Sociedade;

(ii) assegurar que o potencial prestador de serviço tenha capacidade de fornecer o produto/serviço dentro das especificações técnicas bem como garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e informações processados ou armazenados;

(iii) assegurar que o potencial prestador de serviço esteja em condições de cumprir a legislação vigente e fornecer à Sociedade, a qualquer tempo, o acesso aos dados e informações a serem processados ou armazenados;

(iv) assegurar que o prestador de serviço proporcione grau de proteção de dados pessoais adequado ao previsto na legislação de privacidade e proteção de

dados pessoais vigente, oferecendo e comprovando garantias de cumprimento de princípios, dos direitos do titular e do regime de proteção de dados.

(v) assegurar que o potencial prestador de serviço demonstre a identificação e segregação dos dados dos Membros do Mercado Estar, conforme aplicável, por meio de controles físicos ou lógicos, bem como a qualidade dos controles de acessos voltados à proteção de dados e informações;

(vi) quando pertinente, comunicar à CVM a respeito das contratações de serviços relevantes de processamento e armazenamento de dados, bem como quaisquer alterações contratuais relevantes;

(vii) garantir que o contrato firmado entre as partes apresente de maneira clara a adoção de medidas de segurança para transmissão e armazenamento de dados, além da manutenção da segregação de dados e controle de acesso para proteção de informações dos Membros do Mercado Estar, conforme aplicável;

(viii) garantir que o contrato firmado entre as partes apresente de maneira clara as cláusulas, em caso de extinção, que versam sobre a transferência de dados e informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência; e

(ix) observar, quando aplicável, a legislação e regras para transferência internacional adotadas pela legislação de privacidade e proteção de dados pessoais, assim como as normas e diretrizes adotadas pela Autoridade Nacional de Proteção de Dados.

8.2. Configuram exceções à esta Política de Cibersegurança, sem configurar quebra de sigilo ou confidencialidade, o trânsito de informações para o exercício regular de direitos com órgãos e entidades públicas, como a CVM, Receita Federal, Poder Judiciário, Autoridade Nacional de Proteção de Dados, PROCON, representantes da Sociedade devidamente qualificados (incluindo, mas não se limitando, a advogados, auditores e consultores financeiros).

9. MEDIDAS PARA PREVENÇÃO DE ATAQUES CIBERNÉTICOS

9.1. São medidas adotadas para prevenção de ataques ou incidentes cibernéticos na Estar e no Mercado Estar:

(i) no caso de alto acesso ou alta requisição dos recursos do Mercado Estar, os serviços da Estar estão configurados para escalar a aplicação para atender a demanda, garantindo com isso a continuidade do Mercado Estar;

(ii) em caso de desastres naturais no Brasil, todos os servidores serão recriados na região mais próxima dentro de 1 (uma) hora da identificação do referido desastre;

(iii) a camada de rede do Mercado Estar adota o padrão de *Circuit Breaker* para que caso algum serviço de terceiros fique indisponível, o mesmo não ocorra com a totalidade do sistema do Mercado Estar, ou seja, caso haja indisponibilidade de um serviço por breve período, é viabilizado que apenas esta parte do sistema seja afetada e o restante do Mercado Estar continue operando;

(iv) pelo padrão de SLA, caso o sistema de terceiros não seja restabelecido por qualquer razão dentro em até 8 (oito) horas, será acionado o plano de continuidade dos mesmos;

(v) o acesso de todos os Colaboradores ao Mercado Estar é realizado via VPN configurado pelo IP de cada Colaborador;

(vi) o login de todos os Colaboradores aos sistemas críticos do Mercado Estar é realizado com *two fator* (autenticação de dois fatores);

(vii) nenhum Colaborador terá acesso total ao sistema, sendo os acessos fragmentados por áreas de atuação;

(viii) todos os Colaboradores receberão treinamento de cibersegurança no primeiro dia de trabalho na Estar, sendo certo que tal treinamento será realizado novamente no mínimo anualmente;

(ix) a revisão das regras e provisões de *firewall* são revistas trimestralmente;

(x) as chaves de acessos aos serviços de terceiros serão recriadas a cada 6 (seis) meses;

(xi) são realizados *backups* diários para garantir a impotência dos dados em caso de restauração;

(xii) toda comunicação dos sistemas internos do Mercado Estar é realizada por rede privada dentro do Google Cloud;

(xiii) o banco de dados do Mercado Estar conta com *proxy* de rede privado, sendo possível acessá-lo apenas com IPs previamente autorizados;

(xiv) toda a comunicação interna da Estar e do Mercado Estar deverá utilizar o protocolo HTTP, feito com certificado SSL emitidos pelo Google;

(xv) para prevenção de ataque de DDos é adotado na camada de rede externa o mecanismo de *rate limit*, no qual cada IP poderá realizar apenas algumas centenas de requisições no sistema por dia;

(xvi) anualmente deverá ser realizado teste utilizando o framework *Pentest (*teste de penetração) para prevenção de vulnerabilidades;

10. VIGÊNCIA

9.1. Está Política entra em vigor na data de sua aprovação e somente poderá ser modificada por deliberação do Conselho de Autorregulação e poderá ser consultada mediante solicitação à Estar através do e-mail faleconosco@estar.finance.