Ventor Investimentos Ltda.

Política de Segurança da Informação

Atualizado em maio de 2024

CONTEÚDO

1. APRESENTAÇÃO 4
2. FINALIDADE 4
3. PÚBLICO ALVO 4
4. ESTRUTURA ORGANIZACIONAL 4
5. SEGURANÇA E CONFIDENCIALIDADE DAS INFORMAÇÕES 5
   5.1. COMPROMISSO FORMAL DE CONFIDENCIALIDADE 6
6. CONTROLES FÍSICOS E TECNOLÓGICOS 7
   6.1.REDE CORPORATIVA 7
   6.2. DIREITOS DE ACESSO 8
   6.3. SEGREGAÇÃO DAS ATIVIDADES 8
   6.4. DADOS DE CLIENTES 9
7. UTILIZAÇÃO DE *SOFTWARE* 9
8. BACKUP DAS BASES DE DADOS E SERVIDORES 9
   8.1. *BACKUP SITE* 10
   8.2 *NO-BREAKS* 10
9. TELEFONIA 11
10. TREINAMENTO 11
11. POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS 11
   11.1. CONCEITOS E DEFINIÇÕES 11
   11.2. DADOS FORNECIDOS E COLETADOS - FORMA E FINALIDADE 12
   11.3. INFORMAÇÕES SUJEITAS A ESTA POLÍTICA DE PRIVACIDADE 14
   11.4. ACESSO AOS DADOS PELOS TITULARES 14
   11.5. COOPERAÇÃO COM AUTORIDADES REGULADORAS 15
12. POLÍTICA DE SEGURANÇA CIBERNÉTICA (CYBERSECUITY) 15
   12.1.PROGRAMA DE SEGURANÇA CIBERNÉTICA 15
   12.1.1 IDENTIFICAÇÃO DE RISCOS 16
   12.1.1.1 RELACIONAMENTO COM PARTES EXTERNAS 16
   12.1.2 AÇÕES DE PROTEÇÃO, PREVENÇÃO E MECANISMOS DE SUPERVISÃO 17

12.1.3 MONITORAMENTO E TESTES 19

12.1.3.1 *PENETRATION TEST* 19

12.1.3.2 ANÁLISE DE VULNERABILIDADES INTERNA 20

12.1.4. PLANO DE AÇÃO E RESPOSTA A INCIDENTES 20

12.1.5. COMUNICAÇÃO AOS ÓRGÃOS DE ADMINISTRAÇÃO E À SM 22

12.1.6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO NA NUVEM 22

12.1.7. CAPACITAÇÃO, TREINAMENTO E RECICLAGEM 23

12.2. REGRAS DE USO DA ESTRUTURA TECNOLÓGICA 23

13. CONSIDERAÇÕES FINAIS 24

1. APRESENTAÇÃO

A Ventor Investimentos Ltda. (“Ventor”) é uma instituição não financeira cujo objeto é a prestação de serviços de administração de carteira de títulos e valores mobiliários, mais especificamente a gestão de fundos de investimento regulados pela Instrução da Comissão de Valores Mobiliários (“CVM”) nº 175, de 23 de dezembro de 2022, e pela Resolução do Banco Central do Brasil (“Bacen”) nº 4.444, de 13 de novembro de 2015, bem como suas posteriores alterações. De forma acessória atua ainda na distribuição de cotas dos fundos de investimento por ela geridos, conforme facultado pela Resolução CVM nº 21, de 25 de fevereiro de 2021.

2. FINALIDADE

A presente Política de Segurança da Informação (“Política”) tem por objetivos propiciar (i) o tratamento e controle de dados, inclusive, de clientes, visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis; (ii) a segurança cibernética; (iii) as diretrizes para a avaliação da relevância dos incidentes de segurança, incluindo segurança cibernética, e sobre as situações em que clientes afetados devem ser comunicados; e (iv) a contratação de serviços relevantes prestados por terceiros, e assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico, em atendimento ao disposto, especialmente, na Resolução CVM nº 35, de 26 de maio de 2021 (“Resolução CVM nº 35”), e nas demais normas vigentes.

A Ventor almeja que suas regras, procedimentos e medidas de controles internos sejam efetivos e consistentes com a natureza, complexidade e risco das operações realizadas, com base em uma avaliação de risco que leva em consideração:

I. Regras sobre o acesso e controle de pessoas autorizadas e não autorizadas às informações detidas pela Ventor, inclusive nos casos de mudança de atividade dentro da mesma instituição ou desligamento do profissional;

II. Normas específicas sobre proteção da base de dados e procedimentos internos para tratar casos de vazamento de informações detidas pela Ventor, mesmo que oriundos de ações involuntárias; e

III. Regras de restrição ao uso de sistemas, acessos remotos e qualquer outro meio/veículo que contenha informações detidas pela Ventor no exercício de suas atividades.

3. PÚBLICO ALVO

Esta Política aplica-se a todos os sócios executivos, administradores, empregados e estagiários da empresa (“Funcionários”) e aos demais agentes envolvidos, incluindo terceiros contratados (“Colaboradores”), independente de cargo ou função.

4. ESTRUTURA ORGANIZACIONAL

A área de Suporte e Tecnologia é responsável por assegurar a consistência das rotinas e de procedimentos aqui dispostos e por instituir mecanismos de controle e mitigação dos riscos atrelados à segurança da informação.

A área de *Compliance*, com o apoio da área de Suporte e Tecnologia, é a responsável pela elaboração, monitoramento e divulgação das normas previstas nesta Política, de forma a assegurar a efetividade dos procedimentos ora descritos. Suas atribuições regulares são:

I. Entregar a cada Funcionário e Colaborador uma cópia deste documento e solicitar o preenchimento e a assinatura do Termo de Responsabilidade e Compromisso de Adesão às Políticas, Códigos e Manuais ("TC"), assegurando que todos os Funcionários e Colaboradores leram, entenderam e assumiram o compromisso de zelar pela implementação das normas e princípios da Instituição; e

II. Promover a revisão da presente Política, com periodicidade, no mínimo, bienal ou quando houver alteração na regulação referente à proteção de dados e do programa de segurança cibernética, mantendo sempre atualizadas suas avaliações de risco e vulnerabildades, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes.

A Diretora de *Compliance* é a responsável por tratar e responder questões relativas a esta Política, bem como pela implementação e cumprimento de regras, políticas, procedimentos e controles internos estabelecidos pelo Manual de *Compliance* da Ventor, em conformidade com a regulação vigente.

Cabe salientar que a Ventor conta ainda, nas funções não relacionadas ao *core business* da empresa, com o apoio da estrutura da Icatu Holding S.A ("Icatu"), em virtude de Termo de Rateio firmado entre as referidas instituições.

5. SEGURANÇA E CONFIDENCIALIDADE DAS INFORMAÇÕES

Entende-se por sistemas críticos, sob a ótica da presente Politica, todos os computadores, redes e sistemas eletrônicos e tecnológicos que se vinculam aos processos críticos de negócios e que diretamente executam ou indiretamente fornecem suporte a funcionalidades cujo mau funcionamento ou indisponibilidade pode provocar impacto significativo nos negócios.

O uso das informações e sistemas da Ventor é monitorado e os registros decorrentes do seu uso poderão ser utilizados para verificação e evidência da adequação as regras desta Política.

A utilização dos ativos e sistemas, incluindo computadores, telefones, acesso à *web*, impressora, correio eletrônico e *softwares* próprios ou de terceiros deve ser diligente, profissional e ética. Caso algum Funcionário ou Colaborador identifique a conservação inadequada ou a utilização indevida de qualquer ativo (físico ou eletrônico), deve comunicar a ocorrência à área de *Compliance*.

No que tange ao sigilo das informações produzidas, desenvolvidas (incluindo, mas sem limitação, o desenvolvimento de *softwares* próprios), recebidas ou de qualquer modo utilizadas pela Ventor, todos os Funcionários e Colaboradores devem seguir firmemente os princípios abaixo:

I. Estar ciente de que as informações processadas, mantidas ou registradas em áreas de acesso restrito não podem ser transferidas, alteradas ou transmitidas, por qualquer meio, a terceiros, Funcionários ou Colaboradores de outras áreas da empresa, independentemente de seu nível hierárquico, comprometendo-se a manter sigilo absoluto sobre elas e restringir o seu uso às estritas necessidades das funções que exerce;

II. Ser responsável pela guarda, física e digital, dos documentos relativos às suas atividades, certificando-se de que documentos detidos pela Ventor não permaneçam expostos, sendo ao final do expediente trancados devidamente armazenados em gavetas e arquivos;

III. Bloquear os computadores sempre que sair de sua estação de trabalho;

IV. Ter ciência de que a senha de acesso à rede, bem como as senhas de acesso aos diversos sistemas e *softwares* utilizados na Ventor, são pessoais e intransferíveis, devendo ser mantidas em estrito sigilo;

V. Comprometer-se a não acessar informações para as quais não tenha sido autorizado, ou que não estejam relacionadas às suas atividades profissionais;

VI. Não levar material interno para fora do local de trabalho, principalmente informações financeiras, técnicas e relatórios gerenciais sobre as operações da empresa e informações de clientes, ex-clientes e clientes em potencial;

VII. Ser diligente ao acessar remotamente a VPN e aos diretórios da Ventor, estando atendo tanto ao ambiente e pessoas que o circundam como a rede Wi-Fi a ser utilizada;

VIII. Comunicar imediatamente a área de Suporte e Tecnologia em caso de perda ou roubo de dispositivos móveis;

IX. Não efetuar qualquer comentário ou revelação a outros Funcionários, Colaboradores ou a terceiros sobre informações detidas pela Ventor, inclusive conversas de negócios em locais públicos, devendo restringi-las ao contexto de suas práticas profissionais;

X. Estar ciente que todas as ligações telefônicas são ou poderão ser gravadas, arquivadas, incluindo as chamadas desviadas para aparelhos celulares particulares, através de aplicativo contratado previamente instalado, e podem ser utilizadas para eximir dúvidas a respeito das transações efetuadas e processadas, bem como ouvidas para fins de controle interno;

XI. Estar ciente que os e-mails enviados e recebidos por todos os Funcionários ou Colaboradores em ambiente interno e externo são armazenados e estão à disposição da empresa, podendo ser consultados quando se julgar necessário, assim como ocorre com todo o material produzido pelos Funcionários e Colaboradores no âmbito profissional; e

XII. O uso de aparelhos celulares particulares nas atividades relacionadas à empresa, deverá ser feito de forma não sigilosa e cautelosa, sem o tráfego de informações confidenciais ou sensíveis. Além disso, recomenda-se que se evite o uso destes aparelhos durante o expediente, com propósitos extra profissionais.

5.1 COMPROMISSO FORMAL DE CONFIDENCIALIDADE

Os Funcionário e Colaboradores assumem, ao assinar o TC, ter conhecimento do inteiro teor das Políticas, Códigos e Manuais vigentes da Ventor, estar de pleno acordo com suas normas e diretrizes e comprometem-se a cumpri-las fielmente durante toda a vigência de seus contratos, sendo certo que tópicos referentes ao tratamento e comportamento esperado diante de informações confidenciais, reservadas ou privilegiadas estão abordados na presente Política, no Código de Ética e no Manual de *Compliance* da instituição.

Os terceiros contratados pela Ventor e pela Icatu que possuem acesso, no exercício de suas atividades, a informações confidenciais, reservadas ou privilegiadas, apresentam cláusula específica de confidencialidade em seus contratos de prestação de serviço.

Ademais, caberá à área de *Compliance* e a Diretoria da Ventor, em casos de vazamento de informações detidas pela Ventor, mesmo que oriundos de ações involuntárias, avaliar e julgar o ocorrido, podendo inclusive acarretar no desligamento do quadro de Funcionários ou a solicitação de afastamento do Colaborador, sem prejuízo de responder pessoalmente, civil e criminalmente, pela prática de ato ou omissão em desacordo com os termos apresentados.

6. CONTROLES FÍSICOS E TECNOLÓGICOS

A Ventor considera ser de extrema relevância a adoção de procedimentos para que as informações da instituição sejam adequadamente protegidas, sendo eles:

I. Regras mínimas para definição de senhas de acesso a dispositivos corporativos e sistemas de rede;

II. Definição de perfis de acesso às instalações da instituição;

III. Gerenciamento e controle dos acessos, com a possibilidade de revogação de acessos rapidamente quando necessário;

IV. Adoção de procedimentos de replicação de dados e *backup* diário de informações com guarda externa;

V. Eventos de *login* e alteração de senhas auditáveis e rastreáveis;

VI. Criação de *logs* e trilhas de auditoria sempre que facultado pelos sistemas utilizados;

VII. Impossibilidade da utilização por Funcionários e Colaboradores dos acessos USB das estações de trabalho, exceto quando aprovado pela área de *Compliance* ou pela área de Suporte e Tecnologia;

VIII. Espaço físico adequado e seguro para a guarda dos equipamentos;

IX. Restrição de acesso físico das áreas com informações críticas/sensíveis (abertura das portas via identificação biométrica);

X. Segurança e controles de acesso nas instalações de contingência;

XI. Acesso remoto disponível para usuários devidamente identificados e autenticados, bem como, conforme necessário, utilização de conexão criptografada para acesso ao ambiente da instituição de fora desta;

XII. Uso exclusivo de *softwares* e equipamentos homologados pela área de Sistemas e Tecnologia; e

XIII. Utilização de anti-vírus em todas as estações, servidores de arquivos e correio e de *gateway* anti-spam/anti-vírus para todos os e-mails recebidos.

6.1. REDE CORPORATIVA

Todos os usuários da rede corporativa da Ventor são identificados através de um *login name* e uma senha pessoal, intransferível e com prazo de expiração de validade. Assim, antes de acessar quaisquer recursos ou informações disponíveis na rede, o usuário deve identificar-se com seu *login,* autenticar seu acesso através de sua senha pessoal e validar via segundo fator de autenticação.

De acordo com as melhores práticas de segurança da informação, esta senha é alterada periodicamente e todas as tentativas de acesso à rede mal sucedidas, seja de dentro das instalações da Ventor ou através de acesso remoto,

são registradas em *log* e alertadas através de sistema de monitoramento. Após 5 (cinco) tentativas mal sucedidas, a conta do usuário é bloqueada.

Adicionalmente, todas as estações de trabalho e servidores são protegidos por *screen savers*, que bloqueiam o acesso, após 30 (trinta) minutos sem uso.

6.2. DIREITOS DE ACESSO

A estrutura de Sistemas e Tecnologia adota uma política de segurança do tipo fechada, na qual apenas as pessoas e as máquinas autorizadas têm acesso à rede e aos serviços. A rede é protegida por *Firewalls*, visando impedir acessos não autorizados.

A criação/eliminação de usuários e o direito de acesso é realizada por meio do sistema de permissão, denominado Gerenciador de Direitos de Acesso ("GDA"), o qual requer autorização do gerente responsável pela área. A revisão aos acessos lógicos é realizada uma vez por ano.

O sistema GDA gerencia a concessão e revogação de direitos de acesso, aos usuários, a servidores de arquivos de forma discricionária, utilizando o conceito de unidades de acesso, isto é, cada usuário tem mapeado quais servidores e diretórios poderá visualizar e/ou editar.

6.3. SEGREGAÇÃO DAS ATIVIDADES

A Ventor atua apenas na gestão de fundos de investimento e na distribuição de cotas dos fundos por ela geridos, assim, como disposto na norma vigente, não há necessidade de segregação física de suas instalações ou entre os Funcionários da empresa. Entretanto, tal segregação é observada no que tange aos Colaboradores, que realizam as funções não relacionadas ao *core business* da instituição, e principlamente, quanto ao *Data Center* (sala dos servidores e equipamentos de telecomunicações).

Cabe destacar que o *Data Center* é equipado com sistema de segurança composto por câmeras e alarmes, monitorado 24 (vinte e quatro) horas por dia, sendo o acesso permitido apenas mediante verificação de biometria.

Além disso, conta com um sistema contra incêndio FM200, com detecção de fumaça e gás, sistema de refrigeração com monitoramento de máquinas e sistema de energia composto por redundância, *no-breaks* e geradores a diesel.

Almejando a segregação funcional entre as áreas da empresa, como melhor tratado no item 6.2 acima, cada usuário tem mapeado quais servidores e diretórios terá acesso, a fim de evitar potenciais conflitos de interesse e mitigar a ocorrência de ilícitos legais ou contrários à regulação. Neste sentido, vale mencionar que às áreas Comerciais, responsável também pela distribuição de cotas, e de Gestão possuem diretórios e acessos integralmente apartados.

É importante ressaltar que as situações de potenciais conflitos de interesse são também tratadas em documento apartado à presente Política. Assim, para maiores informações, recomenda-se a leitura cuidadosa do Manual de *Compliance*.

6.4. DADOS DE CLIENTES

A Ventor possui regras, procedimentos e controles internos adequados, previstos em sua Política de Privacidade e de Proteção de Dados Pessoais, nos termos do item 11., abaixo, visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações dos clientes.

As informações cadastrais dos clientes são armazenadas em sistemas proprietários, os quais respeitam todas as regras internas supracitadas, por exemplo, GDA, além de um mecanismo de adicional de criptografia.

Caso qualquer informação precise ser compartilhada com outras áreas, os dados dos clientes são criptografados, almejando prevenir o risco de acesso não autorizado, de adulteração ou de mau uso da informação. Apenas os Funcionários previamente autorizados possuem o decodificador de tal ferramenta de segurança.

7. UTILIZAÇÃO DE *SOFTWARE*

A Ventor possui *software*(s) próprio(s), sobre o(s) qual(is) possui(em) propriedade exclusiva, bem como licenças para o uso de *software* provenientes de diversos fornecedores. Exceto quando expressamente autorizado pela Diretora de *Compliance*, nenhum Funcionário ou Colaborador pode reproduzir, copiar ou divulgar quaisquer informações de dados, códigos ou fonte de qualquer *software*, seja ele próprio da Ventor ou proveniente de fornecedores contratados. De acordo com a Lei de Proteção ao Programa de Computador (Lei nº 9609/98, de 19 de fevereiro de 1998), os envolvidos em reprodução ilegal de *software* ficam sujeitos a sanções penais além de responder por perdas e danos.

Somente a área de Suporte e Tecnologia está autorizada a realizar instalações de quaisquer *softwares* ou programas em quaisquer máquinas da Ventor. Desta forma, os Funcionários e Colaboradores comprometem-se a não instalar qualquer *software* ou programa, de qualquer procedência, nos computadores da Ventor, exceto quando expressamente autorizado pelas áreas responsáveis e devem comunicar imediatamente à área de *Compliance*, caso tomem conhecimento de utilização inadequada de *software* ou de sua respectiva documentação nas instalações da Instituição ou utilização não autorizada de *software* da Ventor fora de suas instalações.

Cabe destacar que a área de Suporte e Tecnologia realiza, através de *softwares* específicos ou durante procedimentos de manutenção ou troca das estações de trabalho, inventários periódicos dos *softwares* instalados nas máquinas utilizadas pelos Funcionários e Colaboradores. Através destes relatórios é possível detectar programas não autorizados e tomar as devidas providências.

8. *BACKUP* DAS BASES DE DADOS E SERVIDORES

A Ventor realiza *backup* e a proteção dos dados (servidores de arquivo e bases de dados), através do Sistema Veeam Backup, diariamente em disco rígido e em fitas magnéticas LTO, os dados armazenados em disco rígido são replicados para o Backup Site, fora das instalações da empresa. As informações contidas nos discos rígidos são armazenas por 20 dias. As fitas mensais de janeiro a novembro são guardadas por um ano enquanto a do mês de dezembro, por ser relativa ao fechamento do ano, é preservada por 5 (cinco) anos.

São realizados testes de *restore* nas fitas mensais. Todas as fitas são etiquetadas para proporcionar um controle de modo a evitar o seu uso indevido. Também são atendidas as recomendações dos fabricantes quanto à vida útil das mesmas.

Para maior segurança, as fitas de *backup* são mantidas num cofre resistente a fogo localizado fora das instalações da empresa. O acesso ao cofre é restrito aos funcionários da área de Suporte e Tecnologia e ao *Database Administrator* (DBA) da área de Desenvolvimento.

Procedimentos adicionais de *backup* podem ser realizados em situações específicas como, por exemplo, quando ocorre a limpeza de arquivos de um sistema próprio ou de terceiros. Nesses casos, o *backup* da base de dados poderá ser mantido em fita por um período determinado pelo analista de sistemas responsável.

Por fim, alguns *backups* podem ser armazenados em outro tipo de mídia, por exemplo, unidade de disco externa, conforme a necessidade do usuário e avaliação da área de Suporte e Tecnologia.

8.1 *BACKUP SITE*

A Ventor mantém local para atender de forma contingencial as áreas chaves da empresa, em caso de impossibilidade de utilização do escritório oficial. Assim, além dos procedimentos supracitados, os dados são replicados ao longo do dia para o ambiente contingencial.

Em adição ao monitoramento em tempo real e as visitas mensais para manutenção e verificação do *Backup Site*, a área de Suporte e Tecnologia promove, no mínimo, 2 (dois) testes no decorrer do ano:

I. Teste Técnico: realizado no primeiro semestre de cada ano, verifica as condições de acessibilidade aos sistemas e demais recursos com participação exclusiva dos Colaboradores da área de Suporte e Tecnologia; e

II. Teste de Usuários: realizado no segundo semestre de cada ano, cria as condições que visam simular uma situação real de desastre. Os usuários comparecem ou acessam remotamente ao *Backup Site* e realizam testes, de forma a contemplar os processos críticos de cada área.

Os relatórios gerados a partir dos referidos testes são enviados para o Comitê de Continuidade Operacional - CCO, o qual tem como responsabilidade criar e atualizar o Plano de Contingência Operacional, e ficam devidamente armazenados para eventuais consultas futuras.

Vale registrar que, antes dos testes, o link entre o ambiente principal e o *Backup Site* é intencionalmente "derrubado". Deste modo, as operações realizadas pelos usuários em um ambiente não causam qualquer efeito no outro.

8.2 *NO-BREAKS*

Todos os equipamentos da Ventor, incluindo os servidores, bancos de dados, estações de trabalho e telefonia, estão ligados a sistemas de *no-break,* os quais encontram-se associados a um gerador próprio, o que permite a continuidade dos serviços, inclusive dos *backups* supracitados, no caso da falta de energia, mesmo que por um espaço de tempo prolongado.

9. TELEFONIA

As ligações telefônicas da Ventor são gravadas, inclusive, aquelas redirecionadas para atendimento remoto, no sistema de gravação da OTS - Option Telecom Serviços. O sistema de arquivamento é protegido contra adulterações e permite a realização de auditorias e inspeções.

As gravações são consultadas em caso de dúvidas, inconsistência de dados e/ou discordância de clientes, intermediários e contrapartes. De forma a testar a eficácia do referido sistema de gravação, são selecionadas aleatoriamente duas datas por semestre, nas quais se busca acessar determinadas gravações telefônicas, também randomicamente selecionadas.

10. TREINAMENTO

A Ventor possui programa de treinamento para Funcionários e Colaboradores, visando a conscientização sobre os riscos e relevância das práticas de segurança da informação, principalmente no que se refere as informações confidenciais, reservadas ou privilegiadas.

Cabe à área de *Compliance* determinar a necessidade e periodicidade dos treinamentos, assim como quais pessoas devem estar envolvidas, de acordo com a análise dos riscos a que a empresa esteja exposta, tendo em vista seus serviços, base de clientes e estrutura interna.

11. POLÍTICA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

A presente Política de Privacidade e Proteção de Dados Pessoais ("Política de Privacidade") tem como objetivo orientar quanto às diretrizes aplicáveis à privacidade e proteção dos dados pessoais, em atendimento ao disposto na Lei nº 13.709, de 14 de agosto de 2018 ("Lei Geral de Proteção de Dados Pessoais"), e alterações posteriores, e na Resolução CVM nº 35.
A Política de Privacidade é parte integrante da Política de Segurança da Informação e encontra-se disponível para consulta no *website* da Ventor.

11.1. CONCEITOS E DEFINIÇÕES

Para fins da Privacidade e da Proteção de Dados Pessoais e de acordo com o que determina a Lei Geral de Proteção de Dados Pessoais, são assim definidos:

Titular: pessoa natural identificada ou identificável a quem se referem os dados pessoais que são objeto de tratamento pela Ventor, assim entendidos aqueles fruto de suas atividades, bem como seus Funcionários, Colaboradores e prestadores de serviço.

Dado pessoal: qualquer informação relacionada ao Titular, por exemplo, nome, sobrenome, data de nascimento, documentos pessoais, cookies, endereço IP, entre outros.

Dado pessoal sensível: dado pessoal 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.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. A Ventor pode figurar como Controlador, dependendo do caso.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. A Ventor pode figurar como Operador, dependendo do caso.

Encarregado: pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os Titulares e a Autoridade Nacional de Proteção de Dados (ANPD).

Cabe ao Encarregado - além das atribuições aqui definidas - a responsabilidade por tratar e responder questões relativas a esta Política de Privacidade, bem como pela implementação e cumprimento de regras, políticas, procedimentos e controles internos ora estabelecidos.

Terceiros: pessoa natural ou jurídica que possui relacionamento com a Ventor e, no exercício de suas atividades, possa vir a ter acesso aos dados pessoais referentes aos Titulares.

Agentes de tratamento: o controlador e o operador.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Consentimento: manifestação livre, informada e inequívoca pela qual o Titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

11.2. DADOS FORNECIDOS E COLETADOS - FORMA E FINALIDADE

Conforme supracitado, a Ventor possui como principal objeto a gestão de fundos de investimento e, de forma acessória, a distribuição de tais produtos.

Assim, no âmbito de suas atividades, no que tange aos dados pessoais, a Ventor, em consonância com a abrangência e prazos estabelecidos pela regulação vigente: (i) acessa informações cadastrais de seus cotistas, procuradores, representantes legais e beneficiários finais, quando aplicável, (ii) monitora o saldo em cotas de cada cotista, bem como os dados referentes ao histórico de suas movimentações, (iii) verifica eventuais registros criminais, comerciais e financeiros dos cotistas, Funcionários, Colaboradores e prestadores de serviços, (iv) avalia, enquanto oportunidades de investimentos, empresas e os potenciais riscos do negócio, podendo, inclusive, abarcar dados dos sócios, administradores e representantes de tais empresas, e (v) recebe contato de potenciais investidores, contrapartes, fornecedores ou terceiros e currículos de pessoas físicas interessadas em integrar o seu quadro de Funcionários.

Ressalta-se que a Ventor, no que tange à Política de Privacidade e da Proteção de Dados Pessoais, figurará na condição de Controladora ou de Operadora dos dados pessoais - conforme conceito disposto no item 11.1., acima, dependendo da relação que mantiver com os Titulares destes dados, como consequência das atividades por ela realizadas, podendo tratar, coletar, armazenar e compartilhar com as sociedades sob controle direto ou indireto da Ventor, sempre com a estrita observância à Lei Geral de Proteção de Dados Pessoais, seus dados pessoais e informações cadastrais, financeiras e de operações ativas e passivas e serviços contratados.

Os dados pessoais são coletados por meios éticos e legais e armazenados em ambiente seguro e controlado.

O tratamento de dados pessoais pela Ventor (aí incluídos a coleta, registro, armazenamento, uso, compartilhamento, e eliminação dos dados coletados) têm como finalidade o exercicio de suas atividades fins, diretamente decorrentes de seu objeto social, inclusive o cumprimento de obrigação legal, regulatória, contratual ou interesse legítimo do controlador.

Sem prejuízo, os dados pessoais poderão ser conservados, se sua manutenção for expressamente autorizada por lei ou regulação aplicável, para fins de cumprimento de obrigação legal ou regulatória, transferência a terceiro e no limite prescricional definido em lei para os casos de ingresso de quaisquer ações judiciais e para o exercício de seus direitos em processos judiciais ou administrativos – desde que respeitados os requisitos de tratamento de dados – e uso exclusivo da Ventor.

A Ventor se compromete a tomar todas as medidas cabíveis para manter o absoluto sigilo e a estrita confidencialidade de todas as informações, dados pessoais ou especificações a que tiver acesso ou que porventura venha a conhecer ou ter ciência sobre os Titulares, em razão da prestação dos seus serviços.

Como regra geral, é vedado à Ventor ceder e/ou permitir acesso por pessoas e empresas alheias às informações e dados acima mencionados, ressalvadas as hipóteses de necessária troca destas informações e dados com os Terceiros, definidos no item 11.1., acima, assim entendidos os Administradores Fiduciários dos fundos de investimento geridos e as empresas e Colaboradores da Icatu Holding S/A, que auxiliam a Ventor, via Termo de Rateio, no desempenho de suas atividades.

O acesso de Terceiros às informações coletadas pela Ventor se dá exclusivamente para atendimento das finalidades informadas nesta Política de Privacidade e da Proteção de Dados Pessoais e dentro do limite necessário ao desempenho das atividades relativas ao curso normal dos seus negócios, incluindo, mas não se limitando:

I. Administradores Fiduciários dos fundos, com intuito de efetivação do cadastro e movimentações das pessoas físicas e jurídicas;

II. Demais prestadoras de serviços que executam operações comerciais e/ou de processamento de informações para a Ventor;

III. Auditores independentes;

IV. Agências de cobrança, serviços de proteção ao crédito e assemelhados; e

V. Órgãos reguladores competentes.

Sempre que se fizer necessária a utilização das informações coletadas pela Ventor para outros fins que não os definidos nesta Política de Privacidade ou aquele expressamente autorizado pelo Titular, a instituição informará diretamente ao Titular sobre esta nova finalidade e, quando necessário, coletará uma nova autorização.

Os dados pessoais tratados pela Ventor serão automaticamente eliminados quando deixarem de ser úteis para os fins para os quais foram coletados, ou quando o Titular solicitar expressamente sua eliminação.

11.3. INFORMAÇÕES SUJEITAS À ESTA POLÍTICA DE PRIVACIDADE E DA PROTEÇÃO DE DADOS PESSOAIS

Estão sujeitos à esta Política de Privacidade e da Proteção de Dados Pessoais todos os dados pessoais fornecidos à Ventor ou por esta coletados dos Titulares, conforme definido no item 11.2., acima.

Considerando as atividades desempenhadas por esta instituição, não se vislumbra a coleta ou recebimento de dados pessoais sensíveis, porém, caso haja acesso aos mesmos, a Ventor deverá empregar o tratamento necessário aos dados em questão.

Para fins desta Política de Privacidade e da Proteção de Dados Pessoais, os dados pessoais são classificados em 2 (dois) grupos:

I. Dados pessoais fornecidos pelo Titular: são aquelas inseridos ou encaminhados pelo Titular ou seu representante legal, decorrentes das atividades desempenhadas pela Ventor, em Fichas Cadastrais, Termos de Adesão, Declarações, Contratos, Formulários, entre outros.

II. Dados pessoais coletados do Titular: são aqueles diretamente coletados pela Ventor quando da análise de investimentos ou quando da realização de checagens mandatórias de "conheça seu cliente, Funcionários, Colaboradores e terceiros contratados", e "lavagem de dinheiro", utiilizando-se, para tanto, sites públicos, sites de busca, banco de dados e sistema de checagem de dados.

11.4. ACESSO AOS DADOS PELOS TITULARES

Em cumprimento à legislação aplicável, a Ventor garante ao Titular a possibilidade de apresentação de solicitações baseadas nos seguintes direitos:

I. Confirmação da existência de tratamento;

II. Acesso aos dados;

III. Correção de dados incompletos, inexatos ou desatualizados;

IV. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação;

V. Portabilidade de seus dados a outro fornecedor de serviço ou produto, mediante requisição expressa pelo Titular, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;

VI. Eliminação dos dados tratados com consentimento do Titular, exceto nas hipóteses previstas pela legislação aplicável;

VII. Obtenção de informações sobre as entidades públicas ou privadas com as quais a Ventor compartilhou seus dados;

VIII. Informação sobre a possibilidade de não fornecer o seu consentimento, bem como de ser informado sobre as consequências, em caso de negativa; e

IX. Revogação do consentimento.

Os referidos direitos poderão ser exercidos pelo Titular, por meio do envio de requisição para nosso Encarregado de Proteção de Dados através do endereço de e-mail: encarregadoLGPD@ventorinvestimentos.com.br.

A Ventor empreenderá todos os esforços para atender tais pedidos no menor espaço de tempo possível, no entanto, fatores justificáveis, tais como a complexidade da ação requisitada, poderão atrasar ou impedir seu rápido atendimento.

Por fim, o Titular deve estar ciente que sua requisição poderá ser legalmente rejeitada, seja por motivos formais (a exemplo da incapacidade do Titular de comprovar sua identidade) ou legais (a exemplo do livre exercício do direito à manutenção de dados pela Ventor).

O teor desta Política de Privacidade e da Proteção de Dados Pessoais poderá ser alterado pela Ventor a qualquer momento, conforme a finalidade ou necessidade, cabendo aos Titulares verificá-la sempre que efetuar o acesso ao website da empresa.

11.5. COOPERAÇÃO COM AUTORIDADES REGULADORAS

Nas hipóteses em que se fizer necessária a divulgação dos dados pessoais dos Titulares, seja em razão de cumprimento de lei, determinação judicial ou de órgão competente fiscalizador das atividades desenvolvidas pela Ventor, tais informações deverão ser reveladas somente nos estritos termos e nos limites requeridos para a sua divulgação, sendo que os Titulares das informações divulgadas, na medida do possível, serão notificados sobre tal divulgação, para que tomem as medidas protetivas ou reparadoras apropriadas, quando cabível.

12. POLÍTICA DE SEGURANÇA CIBERNÉTICA (“CYBERSECURITY”)

A presente Política de Segurança Cibernética (“Política de Cybersecutiry”) tem por objetivo prevenir, detectar e reduzir a vulnerabilidade aos riscos e potenciais consequências de ataques cibernéticos, buscando assegurar a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e dos sistemas de informação utilizados pela instituição, em atendimento ao disposto nas Regras e Procedimentos de Deveres Básicos da ANBIMA e no Guia de Cibersegurança da ANBIMA.

12.1. PROGRAMA DE SEGURANÇA CIBERNÉTICA

O programa de segurança cibernética da Ventor almeja que suas regras, procedimentos e medidas sejam efetivos e consistentes com a natureza, complexidade e risco das operações realizadas, com base em uma avaliação de risco que leva em consideração:

I. Identificação/ avaliação de risco: mapear os riscos internos e externos, sejam eles suas vulnerabilidades, assim como possíveis cenários de ameaças, e os ativos e processos que precisam de proteção, como equipamentos, sistemas, dados ou processos;

II. Prevenção e proteção: estabelecer um conjunto de medidas cujo objetivo é mitigar a concretização de ameaças e riscos identificados, ou seja, impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles;

III. Monitoramento e testes: detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico global, mantendo-as em base de conhecimento;

IV. Resposta: ter um plano efetivo de resposta, tratamento e recuperação de incidentes previstos durante a avaliação de riscos, que permita a continuidade dos negócios ou a recuperação adequada em casos mais graves; e

V. Governança: manter o programa continuamente testado e atualizado e reavaliando riscos residuais, garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida.

12.1.1. IDENTIFICAÇÃO DE RISCOS

A área de Suporte e Tecnologia, em conjunto com os gestores das áreas de negócio da Ventor, é responsável por identificar ativos relevantes da instituição. Para tanto, produz-se uma matriz com os processos e sistemas críticos, na quais são apontadas as áreas envolvidas (origem e destino), contemplando, inclusive, quando aplicável, prestadores de serviço terceirizados, incluindo serviços de nuvem, e os recursos necessários para uma correta execução.

Considerando que os ataques cibernéticos podem ser realizados por diferentes agentes, a Ventor, visando proteger os ativos supracitados, dedica especial atenção aos métodos a seguir:

I. *Malware*: *softwares* desenvolvidos para corromper os computadores e redes, como: (i) vírus - *software* que causa danos à máquina, rede, *softwares* e banco de dados; (ii) cavalo de troia - aparece dentro de outro *software* criando uma porta para a invasão do computador; (iii) *spyware* - *software* malicioso para coletar e monitorar o uso de informações; e (iv) *ransomware* - *software* malicioso que bloqueia o acesso aos sistemas e base de dados, solicitando um resgate para que o acesso seja reestabelecido;

II. Engenharia social: métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como exemplo: (i) *pharming* - direciona o usuário para um site fraudulento, sem o seu conhecimento; (ii) *phishing*: *links* vinculados por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais; (iii) *vishing* - simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais; e (iv) acesso pessoal - pessoas localizadas em lugares públicos, a fim de captar qualquer tipo de informação que possa ser utilizada posteriormente para um ataque;

III. Ataques de DDoS (D*istributed Denial of Services*): ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e

IV. Invasões (*Advanced Persistent Threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

12.1.1.1. RELACIONAMENTO COM PARTES EXTERNAS

Os fornecedores, prestadores de serviços e parceiros (“Partes Externas”) podem representar uma fonte significativa de riscos para a instituição. Desta forma, antes de iniciar um relacionamento e durante a sua execução, a Ventor avalia o nível de risco cibernético que tal relação pode representar.

A avaliação acima mencionada engloba a análise, por parte da Ventor, dos controles estabelecidos pelas Partes Externas a respeito da segurança cibernética (se estas possuem políticas internas sobre o tema e sua capacidade de evitar eventuais ataques cibernéticos). Durante este processo, especial atenção é dispensada àqueles que recebem e/ou tratam dados considerados confidenciais ou de clientes, bem como para os que possuem conexões lógicas (*links*) com a instituição.

Conforme necessário e dependendo da avaliação dos riscos, a Ventor poderá solicitar a inclusão de disposições específicas relacionadas ao risco cibernético nos contratos de prestação de serviços.

12.1.2. AÇÕES DE PROTEÇÃO, PREVENÇÃO E MECANISMOS DE SUPERVISÃO

A Ventor, com o objetivo de mitigar a concretização de ameaças cibernéticas, mantém um conjunto de medidas que visam proteger os ativos da instituição, bem como supervisionar os processos de prevenção préviamente definidos, e para tanto utiliza serviço de proteção de email contra spams e malwares.

A empresa utiliza *firewalls*, o qual controla o acesso *web* de entrada e saída, tem sistema de prevenção contra invasões e proteção avançada contra *malware*. O *firewall* também registra todos os eventos suspeitos relacionados ao acesso à rede corporativa através da Internet.

No que tange à segurança do correio eletrônico, a Ventor utiliza Antispam, que filtra todas as mensagens recebidas, evitando a entrega daquelas consideradas maliciosas ou indesejadas, e permite a troca de mensagens criptografadas com endereços de correio eletrônico externos. Na troca de mensagens internas, a Ventor pode utilizar, conforme demanda, a criptografia por certificado digital, compatível com o correio utilizado na empresa.

A Ventor permite que alguns de seus Funcionários tenham acesso condicional ao correio corporativo em seus celulares pessoais. Nestes casos, os referidos celulares pessoais utilizam a tecnologia Workspace One®, que permite o gerenciamento do correio eletrônico, inclusive, em caso de perda ou roubo, bem como são controlados por software de gerenciamento de dispositivos móveis que mantém a separação entre os dados da empresa e os pessoais.

O ambiente de rede e os servidores são monitorados através de console de monitoramento e antivírus, sendo os eventos registrados pela área de Suporte e Tecnologia em tempo real.

Além do monitoramento interno realizado com o antivírus, a Ventor contrata uma empresa especializada em segurança que faz o monitoramento da rede interna, alertando em caso de qualquer comportamento suspeito de ataque a estações e servidores. Este monitoramento é remoto, em tempo real e realizado por meio de relatórios enviados pelos servidores e estações de trabalho a um servidor de gerenciamento, com acesso restrito da empresa contratada.

Existe também um servidor especializado na instalação e atualização de programas e vacinas antivírus em todas as estações de trabalho e servidores da instituição. A área de Suporte e Tecnologia é responsável pelo gerenciamento e monitoramento deste serviço, enviando o instalador para novas estações e servidores, e intervindo manualmente em caso de instalações mal sucedidas.

A área de Suporte e Tecnologia também é responsável (i) pela instalação dos *patches* de segurança das estações de trabalho e servidores por meio do sistema WSUS, de modo a garantir que todas as correções de segurança

sejam aplicadas (para maior segurança, as atualizações são aplicadas sequencialmente, iniciando nas áreas menos críticas, para que possam ser validadas, e finalizando nas áreas mais críticas); e (ii) pelo gerenciamento das atualizações de segurança enviadas pelos fabricantes dos sistemas e softwares instalados, cuja execução ocorre de modo centralizado a partir de um servidor especializado, o System Center, ou individualmente em cada estação, conforme demanda do produto.

O Centro de Processamento de Dados ("CPD") da Ventor é equipado com sistema de segurança composto por câmeras e alarmes, monitorado 24 (vinte e quatro) horas por dia, sendo o acesso permitido apenas mediante verificação de biometria. Além disso, o CPD conta com um sistema contra incêndio FM200, com detecção de fumaça e gás, sistema de refrigeração com monitoramento de máquinas e sistema de energia composto por redundância, *no-breaks* e geradores de energia a diesel.

O *backup* e a proteção dos dados (servidores de arquivo, bases de dados e correio eletrônico) é realizado através do Sistema Veeam Backup, diariamente, em disco rígido e em fitas magnéticas LTO, que são conduzidas a um local fora das instalações da empresa.

Por considerar de extrema relevância a adoção de procedimentos para que as informações da instituição sejam adequadamente protegidas adota-se, ainda, entre outros:

I. Regras mínimas para definição de senhas de acesso com alta complexidade a dispositivos corporativos e sistemas de rede, os quais também possuem autenticação de múltiplos fatores;

II. Definição de perfis de acesso às instalações da instituição;

III. Gerenciamento e controle dos acessos, com a possibilidade de revogação de acessos rapidamente quando necessário;

IV. Eventos de *login* e alteração de senhas auditáveis e rastreáveis;

V. Criação de *logs* e trilhas de auditoria sempre que facultado pelos sistemas utilizados;

VI. Impossibilidade da utilização por Funcionários e Colaboradores dos acessos de CD, DVD e USB das estações de trabalho, exceto quando aprovado pela área de Compliance ou pela área de Suporte e Tecnologia;

VII. Segurança e controles de acesso nas instalações de contingência;

VIII. Acesso remoto disponível para usuários devidamente identificados e autenticados, através de ferramenta com múltiplos fatores de autenticação, bem como, conforme necessário, utilização de conexão criptografada para acesso ao ambiente da instituição de fora desta;

IX. Estações de trabalho são protegidas por *screen savers* após 30 (trinta) minutos sem uso; e

X. Uso exclusivo de *softwares* e equipamentos homologados pela área de Sistemas e Tecnologia, sendo atualizado mensalmente um inventário, a fim de identificar eventuais irregularidades.

Por fim, as contas de Administrador das estações de trabalho têm senhas aleatórias, totalmente desconhecidas, as quais somente podem ser decifradas pela área de Suporte e Tecnologia, através de uma planilha eletrônica de acesso restrito, que calcula o valor da senha por intermédio de um algoritmo específico. Todas as tentativas de acesso à rede mal sucedidas, seja de dentro das instalações da Ventor ou através de acesso remoto, são

registradas em *log* e alertadas através de sistema de monitoramento. Após 5 (cinco) tentativas mal sucedidas, a conta do usuário é bloqueada por 30 (trinta) minutos.

Atualmente as áreas de Suporte e Jurídico, utilizam o sistema de cofre de senhas *Senha Segura* para gestão das senhas administradas pelas áreas em questão.

Cabe destacar que os equipamentos pessoais (*Bring Your Own Device* – BYOD), em caso de trabalho remoto, são utilizados exclusivamente como intermediários para acesso às máquinas físicas individuais localizadas no escritório da Ventor, não havendo circulação de dados profissionais nos mesmos.

Optou-se por este mecanismo para assegurar que todas as regras e processos de *Compliance* permanecem vigentes durante a navegação remota, bem como qualquer vínculo pode ser tempestivamente interrompido como, por exemplo, no caso de furto do aparelho ou desligamento do Funcionário.

12.1.3. MONITORAMENTO E TESTES

A Ventor adota mecanismos de monitoramento e realiza testes periódicos de todas as ações de proteção implementadas, visando garantir a efetividade dos procedimentos estabelecidos. A destacar:

I. Mantém inventário atualizado mensalmente de *hardware*, *software* e sistemas, visando o controle dos recursos dos computadores e a presença de programas não licenciados, inclusive, em momento de acesso e/ou trabalho remoto prolongado;

II. Realiza revisão aos acessos lógicos uma vez por ano, normalmente, em julho, visando assegurar que apenas as pessoas e máquinas autorizadas tenham acesso à rede e aos serviços;

III. Efetua, anualmente, via contratação de empresa especializada, testes de invasão cibernética, a qual avalia a segurança do perímetro e possíveis vulnerabilidades internas da instituição, como melhor detalhado no item 12.2.3.1 abaixo. Ao final da análise, a empresa contratada entrega um relatório informando sobre a ocorrência de incidentes, nível de criticidade e medidas para a correção, que são atendidos de acordo com a criticidade;

IV. Monitora diariamente as rotinas de *backup* e proteção dos dados e realiza testes de *restore* nas fitas mensais;

V. Mantém os sistemas operacionais e *softwares* sempre atualizados, instalando as novas versões tempestivamente, através de um servidor de monitoramento *online*, denominado WSUS da Microsoft® (*Windows Server Update Service*);

VI. Testa o plano de ação e resposta a incidentes periodicamente, como abordado no item 12.2.4 abaixo; e

VII. Analisa *online* os *logs* e as trilhas de auditoria criados, de forma a permitir a pronta identificação de ataques, através da plataforma Splunk, ferramenta de centralização e análise de *logs*.

12.1.3.1 *PENETRATION TEST*

A Ventor realiza, anualmente, o *Penetration Test*, através da contratação de empresa especializada terceirizada, almejando avaliar a superfície de exposição externa e suas vulnerabilidades internas, de forma a proteger as informações chaves do ambiente institucional, por exemplo: (i) informações financeiras; (ii) informações

estratégicas e operacionais; (iii) domain administrator da rede; (iv) credenciais de usuários; (v) PII de Funcionários e Colaboradores (Personally Identifiable Information); e (vi) trade secrets.

Para a execução do *Penetration Test*, considera-se as seguintes atividades:

I. Planejamento das ações e definição de requisitos;

II. Levantamento da infraestrutura física, bem como sua topologia (sob o aspecto de segurança);

III. Preparação da ferramenta para varredura (*scan*) de estações de trabalho, servidores e dispositivos de rede; e

IV. Execução dos *scans* e coleta dos resultados para geração dos relatórios.

Utilizam-se, preferencialmente, mas não exclusivamente, as metodologias de *Black Box*. A destacar:

I. Coleta de informações utilizando ferramentas de busca, serviços na Internet, pesquisas em listas de discussões e fóruns, entre outros;

II. Mapeamento e *footprint* de rede, utilizando ferramentas de varredura para localizar *hosts* ativos, serviços e aplicações nos endereços IPs pertencentes à empresa;

III. Verificação de vulnerabilidades nos controladores de domínio, aplicações e servidores de banco de dados;

IV. Análise e mapeamento da aplicação e dos servidores de aplicação para obtenção de informações sobre a plataforma de desenvolvimento, sistema operacional, versão do serviço *web*, entre outras possíveis informações;

V. Realização de varreduras de rede nos servidores que suportam a aplicação, com técnicas como, por exemplo, varreduras de portas TCP e UDP e identificação de serviços através de *banners*;

VI. Verificação de vulnerabilidades de infraestrutura nos servidores que suportam a aplicação;

VII. Análise de vulnerabilidades na aplicação, incluindo a identificação das seguintes classes: Buffer Overflow, Directory Traversal, Cross Site Scripting, SQL Injection, XML Injection, LDAP Injection, Local / Remote File Include, entre outras;

VIII. Tentativa de obtenção de credenciais válidas de acesso para detectar vulnerabilidades em funcionalidades não disponíveis a usuários não autenticados; e

IX. Exploração das possíveis vulnerabilidades identificadas nas atividades anteriores.

Os relatórios com o detalhamento das atividades realizadas, das eventuais vulnerabilidades e dos riscos identificados, bem como com as recomendações técnicas para tratar as possíveis fragilidades de segurança detectadas, são entregues pela empresa contratada à área de Suporte e Tecnologia, a qual atua tempestivamente na elaboração de um plano de ação buscando minimizar os possíveis riscos apontados.

12.1.3.2 ANÁLISE DE VULNERABILIDADES INTERNA

Realiza-se uma varredura da infraestrutura de tecnologia da empresa com o objetivo de identificar pontos vulneráveis que possam ser explorados por *crackers* com intenção, entre outros, de roubar informações, gerar indisponibilidade nos serviços ou causar outros danos ao ambiente.

A referida varredura é efetuada via ferramenta especializada e compreende as estações de trabalho, os servidores, os dispositivos de rede e todos os demais dispositivos IP (*Internet Protocol*).

12.1.4. PLANO DE AÇÃO E RESPOSTA A INCIDENTES

A Ventor, buscando assegurar a ação tempestiva em caso de incidentes, bem como a continuidade dos negócios e a integridade de informações, em face de situações emergenciais, mantém, conjuntamente com a Icatu, um Plano de Continuidade Operacional ("PCO"), o qual possui como principais características:

I. Estrutura Organizacional: estabeleceu-se um Comitê de Continuidade Operacional ("CCO") cujas responsabilidades são criar, atualizar, gerenciar e ativar o PCO, se necessário for, assim como divulgá-lo amplamente entre Funcionários e Colaboradores. O CCO é constituído pelos gerentes das áreas Administrativa, Suporte e Tecnologia, Controladoria e Tesouraria, Sistemas e Jurídico e Compliance. Adicionalmente, o PCO dispõe sobre os colaboradores-chaves e a sequência que estes devem ser acionados, bem como os telefones celulares dos principais contatos internos e externos;

II. Análise de Risco e Impacto: adota-se estratégia de correlação entre incidentes e o inventário de processos e ativos críticos das áreas de negócios. É realizado o estudo de alternativas, contemplando, entre outros, os recursos necessários (internos e externos), os níveis de abrangência e os tempos para avaliação e retomada, com o intuito de garantir que uma eventual paralisação de processo não ultrapasse o tempo limite para retomada dos serviços; e

III. Principais Recursos: apresenta-se opções para todos os incidentes contemplados, incluindo equipamentos como geradores e *no-breaks* e um ambiente externo (*Backup Site*) com infraestrutura capaz de garantir o processamento e a liquidação das operações em uma eventual paralisação total do ambiente de produção e que respeita todos os controles de acesso e questões de segurança tratados na Política de Segurança da Informação.

O ambiente de contingência é testado 2 (duas) vezes ao ano, de forma a verificar se o PCO está sendo cumprido corretamente e os sistemas de *backup* estão funcionando a contento. Toda a documentação relacionada ao gerenciamento de incidentes e aos testes supracitados são devidamente preservadas por, no mínimo, 5 (cinco) anos e podem ser consultadas sempre que necessário.

A Ventor conta, ainda, com um planejamento de ação em caso de incidentes específicos, conforme abaixo disposto:

I. Estação de trabalho e/ou servidor infectado por vírus: o equipamento é imediatamente retirado da rede corporativa, a fim de evitar novas contaminações e maiores danos, e a área de Suporte e Tecnologia realiza uma investigação sobre a forma de infecção e possibilidade de desinfecção. Caso não apresente mais riscos, o equipamento pode ser instalado novamente na rede corporativa ou pode ser restaurada uma "imagem saudável", em caso de servidor uma vez que estes são virtualizados; e

II. Vulnerabilidade nos equipamentos da rede corporativa: a área de Suporte e Tecnologia aplica os procedimentos de correção conforme orientação do fabricante dos produtos. Se necessário, pode-se contratar consultoria externa especializada para auxílio na resolução do incidente.

É importante ressaltar que as regras ora descritas caracterizam uma versão resumida do PCO da empresa, que é tratado em documento específico, apartado à presente Política de Cybersecutiry, o qual é anualmente revisado pelo CCO e encontra-se disponível para consulta dos Funcionários e Colaboradores da Ventor em diretório da rede interna.

12.1.5. COMUNICAÇÃO AOS ÓRGÃOS DE ADMINISTRAÇÃO E À SMI

A Ventor comunicará tempestivamente, à Superintendência com o Mercado e Intermediários ("SMI"), bem como sua Diretoria, a ocorrência de incidentes relevantes que afetem seus processos, sistemas e ativos críticos e que tenham impacto significativo sobre seus clientes, informando (i) a descrição do incidente, indicando de que forma os clientes foram afetados, (ii) avaliação sobre o número de clientes potencialmente afetados, (iii) as medidas já adotadas ou com a pretensão de adotar, (iv) o tempo consumido na solução do evento ou prazo esperado para que isso ocorra e (v) qualquer outra informação considerada importante.

Ademais, elaborará, para envio subsequente à SMI, relatório final contendo no mínimo (i) a descrição do incidente e das medidas tomadas, informando o impacto gerado por este sobre a operação da Ventor e seus reflexos sobre os dados dos clientes e (ii) os aperfeiçoamentos de controles identificados com o objetivo de prevenir, monitorar e detectar a ocorrência de incidentes de segurança cibernética, se for o caso.

12.1.6. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO NA NUVEM

Quando da contratação de terceiros para prestação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a Ventor deverá, previamente, adotar, de forma documentada, procedimentos que contemplem:

I. A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostos. Para tanto, anteriormente a contratação de qualquer prestador de serviço relevante de processamento e armazenamento de dados e de computação em nuvem, a Ventor deverá observar os procedimentos descritos na Política de Contratação de Terceiros, bem como pomover a (i)avaliação técnica a partir de congressos/fóruns de TI, publicações, entrevistas e análise de resultado com outros clientes e (ii) análise da qualidade no atendimento técnico e comercial, principalmente no pós-venda, a partir de entrevistas e experiência com outros clientes.

II. A verificação da capacidade do potencial prestador de serviço de assegurar:

(i) o cumprimento da legislação e da regulamentação em vigor;

(ii) o acesso da Ventor aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

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

(iv) a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

(v) o acesso da Ventor 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;

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

(vii) a identificação e a segregação dos dados dos clientes da Ventor por meio de controles físicos ou lógicos; e

(viii) a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da Ventor.

Na avaliação da relevância do serviço a ser contratado, a Ventor deverá considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado.

12.1.7. CAPACITAÇÃO, TREINAMENTO E RECICLAGEM

A Ventor entende que uma das maiores dificuldades na implantação de um programa de segurança cibernética é educar os Funcionários e Colaboradores para que se habituem às rotinas e controles como, por exemplo, as restrições à utilização da internet e mídias sociais.

Assim sendo, a Ventor: (i) possui programa de treinamento para Funcionários e Colaboradores, visando a conscientização sobre os riscos e relevância das práticas de segurança, que engloba, quando aplicável, treinamentos a) especiais para recém-contratados e b) intensificados para aqueles que trabalham remotamente e/ou foram vítimas de incidente cibernético; (ii) divulga um conjunto de regras de uso da estrutura tecnológica, que deve ser respeitado por todos os Funcionários e Colaboradores, detalhado no item 12.2 abaixo; (iii) entrega a cada Funcionário e Colaborador uma cópia desta Política de Cybersecutiry e solicita o preenchimento e a assinatura TC, no qual assume-se o compromisso em cumprir o que estiver aqui disposto, bem como nas demais políticas, códigos e manuais da instituição; e (iv) conta com o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética.

Além disso, os Colaboradores da área de Suporte e Tecnologia são incentivados a participar de seminários, fóruns de discussão e qualquer outro tipo de evento acerca do tema, de forma a se manter atualizados com novas vulnerabilidades e ameaças que possam alterar a exposição da Ventor aos riscos avaliados originalmente.

Cabe à área de Suporte e Tecnologia, em conjunto com a área de *Compliance*, determinar a necessidade e periodicidade dos treinamentos e das avaliações regulares, assim como quais pessoas devem estar envolvidas, de acordo com a análise dos riscos a que a empresa esteja exposta, tendo em vista seus serviços, base de clientes e estrutura interna.

12.2. REGRAS DE USO DA ESTRUTURA TECNOLÓGICA

Os Funcionários e Colaboradores da Ventor devem, quando do desempenho diário de suas rotinas, atuar da seguinte maneira no que tange à estrutura tecnológica:

I. Utilizar os ativos e sistemas, incluindo computadores, telefones, acesso à web, impressora, correio eletrônico e *softwares* próprios ou de terceiros de forma diligente, profissional e ética;

II. Não utilizar sítios de relacionamento na rede mundial de computadores, salvo em caráter excepcional e com prévia autorização;

III. Comprometer-se a não utilizar nas instalações da Ventor qualquer equipamento de informática sem a prévia

autorização das áreas de Sistemas e Tecnologia. Os computadores devem possuir apenas os sistemas e *softwares* autorizados e licenciados;

IV. Utilizar o correio eletrônico para assuntos pertinentes ao seu trabalho, cuidando sempre da segurança da informação e de eventuais ameaças cibernéticas;

V. Não enviar informações sensíveis como, por exemplo, senhas e *logins* por correio eletrônico. Informações críticas da empresa ou dados pessoais só devem ser enviados em formato criptografado;

VI. Não clicar em links recebidos, mesmo oriundos de remetentes conhecidos, sem que haja clareza do conteúdo a que se refere. É sempre indicado que se escreva o endereço diretamente no *browser;*

VII. Certificar-se antes de acessar qualquer site se este é seguro, por exemplo, através de duplo clique sobre o cadeado ou acede pelo endereço (URL) iniciado por "https://";

VIII. Utilizar os eventuais equipamentos colocados à disposição dos Funcionários e Colaboradores, como, por exemplo, celulares e laptops, de forma diligente, com especial atenção ao uso de redes públicas de *wi-fi*;

IX. Ter ciência de que a senha de acesso à rede, bem como as senhas de acesso aos diversos sistemas e *softwares* utilizados na Ventor, é pessoal e intransferível, devendo ser mantidas em estrito sigilo;

X. Não salvar as senhas de acesso de forma automática nos sistemas e *softwares*; e

XI. Bloquear os computadores sempre que sair de sua estação de trabalho.

13. CONSIDERAÇÕES FINAIS

A área de *Compliance* poderá, a qualquer momento e sem aviso prévio, verificar o conteúdo das ligações telefônicas gravadas, dos arquivos disponíveis no diretório interno e dos e-mails enviados e recebidos pelos Funcionários e Colaboradores, sem que isto configure quebra de sigilo, com vistas ao cumprimento das normas internas estabelecidas. Da mesma forma, poderá proceder nos casos de eventuais equipamentos colocados à disposição dos Funcionários e Colaboradores, como, por exemplo, celulares, laptops e rádios.

Cada Funcionário e Colaborador é responsável por seus atos, comportamento e conduta. Assim, em caso de dúvidas quanto às diretrizes expostas nesta Política ou questionamentos práticos que porventura possam surgir, os mesmos devem ser sanados imediatamente junto à área de *Compliance*.

Além disso, todo Funcionário ou Colaborador que souber ou tiver motivos para acreditar que uma norma, ou qualquer disposição ora apresentada, esteja sendo violada, deve comunicar este fato imediatamente à área de *Compliance*. As notificações podem ser encaminhadas por e-mail ou via telefone, e em todos os casos serão tratadas com total sigilo.

Caberá à área de *Compliance* avaliar e julgar as eventuais solicitações excepcionais que venham a ser apresentadas, sempre formalmente, pelos Funcionários ou Colaboradores.

Os Funcionários e Colaboradores devem ter ciência de que o descumprimento desta Política pode resultar em penalidades a serem estabelecidas, caso a caso, pela área *Compliance* e a Diretoria da Ventor, podendo inclusive acarretar no desligamento do quadro de Funcionários ou a solicitação de afastamento do Colaborador, sem prejuízo de responder pessoalmente, civil e criminalmente, pela prática de ato ou omissão em desacordo com os termos apresentados.