POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS

VGR GESTÃO DE RECURSOS LTDA.
("Sociedade")

Versão Vigente: 01/07/2022

CAPÍTULO I DO OBJETIVO

1.1. O presente instrumento tem como objetivo precípuo a definição de regras e princípiosnorteadores das condutas dos colaboradores da Sociedade, assim entendidos seus (i) sócios; (ii) diretores; (iii) funcionários; (iv) estagiários; ou (v) de quaisquer pessoas que,em virtude de seus cargos, funções ou posições na Sociedade, tenham acesso a informações relevantes sobre a Sociedade, seus negócios ou clientes, em especial no quese refere à segurança da informação e segurança cibernética.

1.2. Os colaboradores atestam a ciência e adesão acerca dos procedimentos definidos pela presente Política mediante assinatura de termo próprio, sendo submetidos anualmente ao Programa de Treinamento adotado pela Sociedade, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

1.3. A Sociedade coletará Termo de Confidencialidade de quaisquer terceiros contratadosque tiverem acesso às informações confidenciais a respeito da Sociedade, seus colaboradores, fundos sob gestão e investidores, salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação deServiços.

1.4. A fim de cumprir o seu objetivo, esta Política será revisada no mínimo a cada 2 (dois)anos, sendo mantido o controle de versões, e circulada aos colaboradores para conhecimento e assinatura do Termo de Adesão e Confidencialidade supramencionado sempre que alterado.

1.5. Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto ao Diretor de Compliance da Sociedade, devendo as questões de seguança cibernética serem tratadas com o responsável pela Tecnologia da Informação.

CAPÍTULO II
PROTEÇÃO DE DADOS PESSOAIS

2.1. O presente Capítulo visa regular o tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Sociedade, assim considerada toda operação realizada com tais dados, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2.2. Considera-se "Dados Pessoais" qualquer informação relacionada a pessoa natural identificada ou identificável. Deste modo, sujeitam-se à tutela desta Política todos os Dados Pessoais de colaboradores, investidores, parceiros, prestadores de serviço ou quaisquer terceiros com os quais a Sociedade mantenha relacionamento de qualquer natureza.

2.2.1. São considerados, ainda, Dados Pessoais aqueles utilizados para formação de perfil comportamental de determinada pessoa natural, se identificada.

2.3. Consideram-se "Dados Pessoais Sensíveis" os Dados Pessoais que versem sobre a 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 vinculados a uma pessoa natural.

2.4. Todos os Dados Pessoais ou Dados Pessoais Sensíveis são informações confidenciais e devem ser tratados como tal para os fins desta Política e demais manuais e políticas internas adotadas pela Sociedade.

2.5. As atividades de tratamento de Dados Pessoais e Dados Pessoais Sensíveis deverão observar a boa-fé e os seguintes princípios:

(i) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

(ii) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

(iii) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

(iv) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus Dados Pessoais;

(v) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de

acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

(vi) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

(vii) segurança: utilização de medidas técnicas e administrativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

(viii) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de Dados Pessoais;

(ix) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

(x) responsabilização e prestação de contas: demonstração, pela Sociedade, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de Dados Pessoais e, inclusive, da eficácia dessas medidas.

2.6. O tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Sociedade só será realizado nas seguintes hipóteses:

(i) para o cumprimento de obrigação legal ou regulatória pela Sociedade;

(ii) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

(iii) quando necessário para atender aos interesses legítimos da Sociedade ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos Dados Pessoais e Dados Pessoais Sensíveis;

(iv) mediante o fornecimento de consentimento pelo titular por escrito ou outro meio que demonstre a manifestação de vontade do titular; ou

(v) para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

2.6.1. O legítimo interesse da Sociedade indicado no item 2.6. (iii) acima poderá ter fundamento, mas não se limita, às seguintes finalidades:

(i) apoio e promoção de atividades da Sociedade; e

(ii) proteção, em relação ao titular, do exercício regular dos seus direitos ou prestação de serviços que o beneficie, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais.

2.6.1.1. No caso de interesse legítimo da Sociedade, somente os Dados Pessoais e Dados Pessoais Sensíveis estritamente necessários serão tratados, sendo outorgada ampla transparência ao titular sobre o tratamento implementado.

2.6.2. O consentimento de que trata o item 2.6 (iv) deve observar as seguintes diretrizes:

(i) se outorgado por escrito deverá constar de cláusula destacada das demais cláusulas contratuais;

(ii) o Dado Pessoal obtido mediante consentimento do titular só poderá ser compartilhado com terceiros se houver expressa autorização do titular;

(iii) o consentimento deve referir-se a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados. Caso alterada a finalidade, deverá ser coletado novo consentimento do titular;

(iv) o consentimento poderá ser revogado a qualquer tempo por manifestação expressa do titular, por procedimento gratuito e facilitado, ratificado o tratamento realizado ao amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação dos dados.

2.7. A Sociedade outorgará ao titular o direito ao acesso facilitado às informações sobre o tratamento de seus dados, que serão disponibilizadas de forma clara, adequada e ostensiva, incluindo as seguintes informações:

(i) finalidade específica do tratamento, ratificando que o tratamento de Dados Pessoais é condição para o fornecimento do serviço de gestão profissional de recursos em virtude de obrigação regulatória;

(ii) forma e duração do tratamento, observados os segredos comercial e industrial;

(iii) identificação e informações de contato da Sociedade que atuará como controladora da informação;

(iv) informações acerca do potencial compartilhamento de dados pela Sociedade e a sua finalidade;

(v) responsabilidades dos colaboradores que realizarão o tratamento; e

(vi) Informações sobre os direitos do titular, na forma do art. 18 da Lei Geral de Proteção de Dados, e meios pelos quais tais direitos poderão ser exercidos.

2.8. O término do tratamento de Dados Pessoais e Dados Pessoais Sensíveis ocorrerá nas seguintes hipóteses:

(i) verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

(ii) fim do período de tratamento, ou seja, 05 (cinco) anos após a cessação da prestação de serviço ao titular;

(iii) comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, resguardado o interesse público; ou

(iv) determinação da autoridade nacional, quando houver violação da Lei Geral de Proteção de Dados.

2.9. Os Dados Pessoais e Dados Pessoais Sensíveis serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

(i) cumprimento de obrigação legal ou regulatória pela Sociedade;

(ii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos acima; ou

(iii) uso exclusivo da Sociedade, vedado seu acesso por terceiro, e desde que anonimizados os dados.

2.10. A Sociedade manterá registro das operações de tratamento de Dados Pessoais e Dados Pessoais Sensíveis que realizar, especialmente quando baseado no seu legítimo interesse.

2.11. A Autoridade Nacional de Proteção de Dados poderá determinar que a Sociedade elabore um relatório de impacto à proteção de Dados Pessoais, inclusive Dados Pessoais Sensíveis, referente às operações de tratamento de dados. Este relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise da Sociedade sobre estas medidas, salvaguardas e mecanismos de mitigação de risco adotados.

2.12. O encarregado pelo tratamento de Dados Pessoais e Dados Pessoais Sensíveis será o Diretor de Compliance da Sociedade. As informações para contato do encarregado estarão disponíveis no site da Sociedade.

CAPÍTULO III
PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

I. ACESSO RESTRITO

2.1.1. A troca de informações entre os colaboradores da Sociedade deve sempre pautar- se no conceito de que o receptor deve ser alguém que necessita receber tais informações para o desempenho de suas

atividades e que não está sujeito a nenhuma barreira que impeça o recebimento daquela informação. Em caso de dúvida a área de compliance deveser acionada previamente à revelação.

2.1.2. Os colaboradores da Sociedade que tiverem acesso aos sistemas de informação serão responsáveis por tomar as precauções necessárias de forma a impedir o acesso não autorizado aos sistemas, devendo salvaguardar as senhas e outros meios de acesso aos mesmos.

2.1.3. Os arquivos da Sociedade são armazenados em nuvem e servidores internos.

2.1.4. O acesso controlado às pastas e arquivos se dá mediante a outorga de senhas de acesso individuais e intransferíveis que permitem a identificação do seu usuário, afastando a utilização das informações ali contidas por pessoas não autorizadas.

2.1.5. Adicionalmente, todas as mensagens enviadas/recebidas dos computadores disponibilizados pela Sociedade permitem a identificação do seu remetente/receptor.

2.1.6. O acesso remoto pelos colaboradores é protegido por senha, pois o sistema se baseiana identidade do usuário, solicitando uma identificação – caso essa pessoa não tenha autorização para acesso, o documento não será exibido.

2.1.7. O armazenamento de informações protegidas em dispositivos portáteis deverestringir-se aqueles fornecidos pela Sociedade.

2.1.8. A outorga e cancelamento de senhas é de responsabilidade da área de Compliance,

sempre mediante orientação do Diretor de Compliance, a quem compete a verificação daestrutura de governança da Sociedade, a fim de evitar a transgressão de barreiras de informação e potenciais conflitos de interesse. Este procedimento deverá ser observado ainda na hipótese de mudança de atividade/área de um determinado profissional dentro da Sociedade.

2.1.9. As senhas de acesso possuem prazo de validade e requisitos mínimos de segurança,devendo ser desabilitadas após um número máximo de tentativas malsucedidas de acesso, sendo esta atividade registrada pelos controles de tecnologia da informação.

2.1.10. Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Sociedade expiram, usando um protetor de tela protegido por senha que exija que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticadonovamente.

2.1.11. No caso do desligamento ou saída de algum colaborador, o acesso aos arquivos será automaticamente bloqueado e a respectiva senha revogada. Para sistemas externos, a Sociedade deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

2.1.12. O controle do acesso a arquivos confidenciais em meio físico é garantido atravésda segregação física da equipe de gestão de recursos de terceiros.

II. BACK-UP

3.2.1 Todos os documentos arquivados nos computadores da Sociedade são objeto de back-up diário com controle das alterações promovidas nos arquivos, garantindo a segurança dos respectivos conteúdos e eventual responsabilização.

3.2.2. O prestador de serviço na nuvem armazena versões anteriores de arquivos por até 90 dias, ou seja, se algum arquivo for apagado ou alterado de forma errônea, é possível recuperá-lo durante este período.

3.2.3.

Além da segurança proporcionada pelo armazenamento na nuvem, diariamente, é efetuado back-up automático de todos os arquivos criados ou alterados ao longo do dia de trabalho através de software especializado. As cópias de back-up são armazenadas, sendo possível o acesso destas mídias em caso de contingência, mediante autorização da área de Compliance.

3.2.4. Os e-mails excluídos são mantidos na Lixeira por 180 dias. Após este período, a mensagem será excluída e somente o administrador poderá recuperá-la através da consolede administração. Neste caso, serão mais 60 dias até que a mensagem seja definitivamenteexcluída sem a possibilidade de recuperação.

III. CÓPIA DE ARQUIVOS E INSTALAÇÕES

2.3.1. Todos os programas de computador utilizados pelos colaboradores devem ter sidopreviamente autorizados pelo responsável pela área de informática. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

2.3.2. A cópia de arquivos e instalação de programas em computadores deverá respeitar os direitos de propriedade intelectual pertinentes, tais como licenças e patentes.

2.3.3. É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede e circulem em ambientes externos com estes arquivos, salvo se em prol da execução e do desenvolvimento dos negócios e dos interesses da Sociedade. Nestes casos, o colaboradorque estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

2.3.4. Qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois pode conter informações restritas e confidenciais mesmo no ambiente interno da Sociedade. É vedada, ainda, a manutenção destes em mesas, máquinas de fax ou copiadoras.

IV. DESCARTE DE INFORMAÇÕES

3.4.1. O descarte de informações confidenciais deve observar as seguintes diretrizes:

(i) o conteúdo descartado deverá ser apagado e/ou as mídias devem ser destruídas, impossibilitando a sua recuperação, de modo que a informação não fique vulnerável a acesso não autorizado;

(ii) os documentos físicos que contenham informação protegida devem ser trituradosimediatamente após seu uso de maneira a evitar sua recuperação ou leitura;

(iii) a eliminação ou a destruição final das mídias ou documentos, realizada por terceiros, deve ser documentada;

(iv) dispositivos de memória e dispositivos de armazenamento (por exemplo laptops, dispositivos USB, discos rígidos portáteis, tablets, smartphones) desativados pelaSociedade devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

V. REDUNDÂNCIA

2.5.1. Além das cópias de segurança acima, outros recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho, a equipe-chave, previamente designada e treinada para tanto, poderá acessar as informações na nuvem dequalquer local.

2.5.2. Para garantir o funcionamento da rede e a integridade dos dados, mesmo na eventual interrupção do fornecimento de energia elétrica, todas as estações de trabalho eo servidor estão conectados a um equipamento do tipo *no-break*, que permite a continuidade do funcionamento da rede por tempo suficiente para que os usuários salvemseus arquivos.

CAPÍTULO IV SUPORTE E MONITORAMENTO

3.1. Em caso de pane da rede ou em alguma estação de trabalho, o fato deverá ser imediatamente comunicado à área de Compliance, que assegurará o suporte interno ou providenciará que seja acionado o suporte externo necessário.

3.2. O sistema eletrônico utilizado pela Sociedade está sujeito à revisão e monitoramentoa qualquer época sem aviso ou permissão, de forma a detectar qualquer irregularidade na transferência de informações, seja interna ou externamente.

3.3. Nesse sentido, tendo em vista que a utilização do e-mail se destina exclusivamente para fins profissionais, como ferramenta para o desempenho das atividades dos colaboradores, a Sociedade também poderá monitorar toda e qualquer troca, interna ou

externa, de e-mails dos colaboradores.

3.4. Qualquer suspeita ou conhecimento de violação desta Política ou incidente de segurança da informação deve ser objeto de informação ao Compliance para que sejam tomadas as devidas providências com relação à apuração dos fatos, mitigação de eventuais riscos, implementação de procedimentos corretivos e responsabilização dos envolvidos.

3.5. Periodicamente e sem aviso prévio, poderão ser realizadas inspeções nos computadores para averiguação de downloads impróprios, não autorizados ou gravados em locais indevidos.

Tratamento de casos de vazamento de informações confidenciais

3.6. No caso de vazamento de informações confidenciais relacionadas aos clientes da Sociedade, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará osinteressados sobre o ocorrido.

3.7. Sem prejuízo, a Sociedade acionará o seu Plano de Recuperação visando a identificação da causa que ensejou o vazamento e responsabilização do causador. Ademais, será elaborado um Relatório acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadas normalmente.

3.8. Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

Firewall

3.9. A Sociedade faz o uso da tecnologia de Firewall para proteger sua rede contraameaças externas.

Rede Wireless

3.10. A Sociedade possuí rede WIFI distinta para uso dos visitantes. Jamais deve ser

divulgada a senha de acesso interno para os visitantes. Os visitantes devem sempresolicitar a senha de acesso para a recepcionista.

3.11. A rede WIFI para visitantes é bloqueada para acessar recursos internos.

Testes de Segurança

3.12. São realizados os seguintes testes de segurança para monitoramento dos sistemasutilizados:

ROTINAS OPERACIONAIS	PERIODICIDADE
Varredura de antivírus	Tempo real
Controle de conteúdo de Internet pelo Firewall e Antivírus	Tempo real
Varredura de memória pelo Antivírus	Tempo real
Autenticação de rede	Tempo real
Bloqueio de tela do Windows por Inatividade	A cada 10 minutos
Backup Online	Diário
Back Up Servidor	Diário
Atualizações nas estações de trabalho	Mensal
Troca da senha dos usuários	Trimestre

CAPÍTULO V
IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

4.1. Considerando a atividade de gestão profissional de recursos de terceiros desempenhada pela Sociedade são essenciais todos os recursos tecnológicos necessáriosao **processo de análise, investimento e desinvestimento**, tais como: (i) disponibilizaçãodas informações diárias sobre os fundos sob gestão; (ii) boletagem de operações; (iii) compra e venda de ativos para as carteiras sob gestão; (iv) conferência e liberação das carteiras diárias dos fundos sob gestão; e (v) acesso aos sistemas de informação. São estes:

A Extranet do Administrador, onde são extraídas as informações referentes a Fundos é protegido por senha individual, com restrições de acesso a cada usuário impostas e monitoradas pelo Diretor de Compliance.

4.2. Abaixo são descritos os riscos internos identificados e respectivas avaliações. Para tanto, considerou-se: (i) possíveis ameaças; (ii) grau de exposição dos ativos supramencionados às ameaças; (iii) impactos financeiros, operacionais e reputacionais; e
(iv) a expectativa de que o evento de segurança se efetive:

Risco Interno	Avaliação Inicial
Utilização de maneira imprópria dos sistemas de informação	*Caso consigam a senha de pessoas com nível de extrema importância para a gestão dos recursos da Sociedade, pode ser possível que, de má fé, venham a ter todas as informações dos fundos geridos pela Sociedade. Ademais, também seria possível a total exposição dos ativos sob gestão da Sociedade, que poderia resultarem um impacto financeiro e reputacional de alto grau para a Sociedade. O evento teria baixa probabilidade de ocorrer, dado que as senhas são pessoais e intransferíveis e todos os procedimentos de segurança para o acesso a esses sistemas são de alto grau de confiabilidade.*

Risco Externo	Avaliação Inicial

Acesso de hackers aos sistemas.	*Caso ocorra a falha de segurança de hackers aos nossos arquivos em nuvem teria um alto impacto na Sociedade, dado que todos os arquivos estão armazenados nesses servidores. Não teria um impacto financeiro alto, pelo fato de não ter arquivos que possibilitem a atuação direta na gestão dos recursos geridos pelaSociedade, porém, poderia ter um impacto reputacional de grau médio. Baixa probabilidade do evento ocorrer, dado que o servidor que usamos é disponibilizado por uma grande empresa de tecnologia que até os dias atuais não tivemos notícias que ocorreu o evento supramencionado a nenhum de seus clientes.*

CAPÍTULO VI
AÇÕES DE PROTEÇÃO E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

5.1. Os planos de ação e prevenção descritos neste Capítulo tem por objetivo mitigar e minimizar a possibilidade de ocorrência de um ataque cibernético, na tentativa de evitar que os riscos identificados se concretizem.

5.2. Neste sentido, a Sociedade ratifica a adoção de controles de acesso físico e lógico implementados em linha com a Política de Segurança da Informação adotada. Tais controles visam a identificação, autenticação e autorização de acesso pelos usuários a sistemas ou ativos da Sociedade, evitando o acesso por terceiros não autorizados.

5.3. Isto posto, todos os colaboradores devem observar de forma estrita as rotinas relacionadas à definição de senhas de acesso aos sistemas e rede, bem como às barreirasda informação com relação a outras atividades desempenhadas pela Sociedade ou empresas do mesmo grupo econômico.

5.4. Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquerinconsistência ou inadequação com relação aos acessos recomendados pelo Diretor de Compliance reportados imediatamente. Especial atenção deverá ser envidada aos casos de desligamento ou gozo de férias de colaboradores.

5.5. São adotadas as seguintes medidas preventivas para cada risco identificado:

Risco Interno	Ação de Proteção/Prevenção
Utilização de maneira imprópria dos sistemas.	*Adotamos a autenticação do usuário, com as devidas permissões para cada colaborador de acordo com seu nível e demandas. As senhas de cada colaborador são intransferíveis, tendo esses suas permissões e entradas nos sistemas monitoradas diretamente pelo Diretor de Compliance*

Risco Externo	Ação de Proteção/Prevenção
Acesso de hackers aos sistemas	*Diligência na contratação dosprestadores de serviço, com uma minuciosa pesquisa sobre os prestadores de serviço de sistemas e suas possíveis falhas, com contratos com claras cláusulas de confidencialidade. Ademais, é utilizado pela Sociedade firewalls e anti-malware em todos os computadores.*

5.6. Todos os novos equipamentos e sistema instalados na Sociedade devem contar comas configurações de proteção acima descritas, sendo realizado teste em ambientes de homologação e de prova antes do início da sua utilização. Sem prejuízo, anualmente são realizadas inspeções visando a verificação da atualização dos sistemas operacionais e softwares instalados nos computadores da Sociedade.

5.7. Todos os programas de computador utilizados pelos colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática, sendo vedadas aplicações não autorizadas por meio de controles de execução de processos. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

CAPÍTULO VII
MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

6.1. São realizados os seguintes testes de verificação para fins de identificação deanomalias, detecção de ameaças, acessos, componentes ou dispositivos não autorizados:

Rotina	**Periodicidade**
Back-up	*Diário*
Teste de restauração de dados	*Diário*
Teste de invasão externa e phishing	*Diário*

Teste de resposta a incidentes com simulação de cenários	*Semestralmente*

6.2. São mantidos inventários atualizados de hardware e softwares utilizados pela Sociedade. Semestralmente são realizadas verificações, a fim de identificar elementos estranhos à Sociedade, tais como computadores não autorizados ou softwares não licenciados.

6.3. Sempre que houver alteração relevante na estrutura tecnológica da Sociedade serão realizadas análises de vulnerabilidade.

CAPÍTULO VIII
RESPOSTAS A INCIDENTES CIBERNÉTICOS

7.1. A Sociedade adota os seguintes planos de ação de resposta a incidentes em função das ameaças identificadas:

Ameaça Interna	Severidade (Classificação)	Plano de Ação
Utilização de maneira imprópria dos sistemas.	*Alto risco*	Identificação de acesso e providências a serem discutidas pela Diretoria.

Ameaça Externa	Severidade (Classificação)	Plano de Ação
Acesso de hackers aos sistemas.	*Grau médio*	Contato direto do Diretor de Compliance com o prestador de serviço do sistema que foi invadido para que sejam medidos os danos e sejam discutidas as possibilidades de reparação.

7.2. Compete à Equipe de Compliance e Risco a comunicação da contingência aos demais colaboradores da Sociedade, orientando-os sobre a postura e providências cabíveis, de acordo com a natureza e severidade da contingência, em observância do Plano de Continuidade de Negócios.

7.3. Cabe à Equipe de Compliance e Risco desenvolver relatórios acerca dos danos ocorridos, percentual das atividades afetadas, impactos financeiros, sugerindo ainda medidas a serem tomadas de modo a possibilitar que as atividades voltem a ser executadasnormalmente. Tais relatórios deverão ser submetidos à Diretoria da Sociedade que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

7.4. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade,a Sociedade estudará procedimentos preventivos a serem implementados e incluídos nesteplano de continuidade de negócios.

CAPÍTULO IX PROGRAMA DE TREINAMENTO

9. A Sociedade conta com um programa de treinamento dos colaboradores que tenham acesso a informações confidenciais, na forma descrita em seu Código de Ética e Conduta. O treinamento levará em consideração o tratamento das informações confidenciais e, no que se refere ao tratamento de Dados Pessoais e Dados Pessoais Sensíveis, abordará aspectos como: (i) natureza; (ii) escopo; (iii) finalidade; (iv) probabilidade e a gravidade de riscos; (v) benefícios decorrentes do tratamento de dados.

9.1Os procedimentos e rotinas definidos na presente Política serão abordados em treinamento anual, coordenado pelo Diretor de Compliance ou terceiro contratado para esta finalidade, visando a sua disseminação entre a equipe da Sociedade.

9.2 Poderão ser promovidos treinamentos em periodicidade menor, visando a atualizaçãoe ampliação do conhecimento dos colaboradores, em especial em virtude de mudanças relevantes nos procedimentos e controles descritos nesta Política.

CAPÍTULO X DISPOSIÇÕES GERAIS E *ENFORCEMENT*

10.1. Todos os documentos, relatórios e informações relevantes para os procedimentos e rotinas descritos nesta Política são arquivados em meio físico ou eletrônico na Sociedade,pelo prazo mínimo de 5 (cinco) anos.

10.2 O presente Instrumento prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os colaboradores da Sociedade aos seus termos e condições.
10.3. A título de *enforcement*, vale notar que a não observância dos dispositivos da presentePolítica resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis ecriminais