POLÍTICA DE SEGURANÇA DA INFORMAÇÃO, SEGURANÇA CIBERNÉTICA e PROTEÇÃO DE DADOS PESSOAIS

Versão vigente: julho/2023
Versão anterior: julho/2022

CAPÍTULO I
DAS DEFINIÇÕES

1.1. São definições importantes para o presente instrumento:

Empresa: significa todos as empresas sob controle comum do grupo, tais como: HMC ITJ Participações Ltda., HMC ITJ Holding Patrimonial Ltda., Gama Investimentos Ltda. e HMC Capital Advisors Consultoria Financeira Ltda.

Colaborador(es): significam todos aqueles que tenham vínculo empregatício, participação societária ou vínculo contratual com Empresa, incluindo os seus sócios.

Terceiro(s): Inclui toda e qualquer pessoa física ou jurídica não pertencente à Empresa, que atuem, direta ou indiretamente, de qualquer forma, em nome de qualquer Empresa, incluindo, mas não se limitando a prestadores de serviço, parceiros de negócio, consultores, distribuidores, representantes, representantes comerciais, mandatários, procuradores, fornecedores, despachantes.

Manual: esta Política de Segurança da Informação, Segurança Cibernética e Proteção de Dados Pessoais.

CAPÍTULO I
DO OBJETIVO

2.1. A presente Política de Segurança da Informação e Segurança Cibernética tem como objetivo precípuo a definição de regras e princípios norteadores das condutas dos Colaboradores no que se refere à segurança da informação, segurança cibernética e proteção de dados pessoais.

2.2. 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 Empresa, a fim de que sejam orientados sobre as rotinas a serem observadas no desempenho dos processos descritos nesta Política.

2.3. A Empresa, por meio do Departamento de Compliance, coletará Termo de Confidencialidade de quaisquer terceiros contratados que tiverem acesso às informações confidenciais a respeito da Empresa, seus Colaboradores, clientes e e fundos de investimento sob gestão (no caso da Gama Investimentos Ltda.), salvo se este compromisso já tiver sido firmado entre as partes mediante a assinatura do correspondente Contrato de Prestação de Serviços.

2.4. 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.

2.5. Em caso de dúvidas ou necessidade de aconselhamento, o colaborador deve buscar auxílio junto ao Departamento de Compliance, devendo as questões de segurança cibernética serem tratadas com responsável pela área de Tecnologia da Informação.

CAPÍTULO III
PROTEÇÃO DE DADOS PESSOAIS

3.1. O presente Capítulo visa regular o tratamento de Dados Pessoais e Dados Pessoais Sensíveis pela Empresa, 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.

3.2. 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, clientes, parceiros, prestadores de serviços ou quaisquer Terceiros com os quais a Empresa mantenha relacionamento de qualquer natureza.

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

3.3. 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.

3.4. 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 Empresa.

3.5. 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 Empresa, 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.

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

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

(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 Empresa 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.

3.6.1. O legítimo interesse da Empresa indicado no item 3.6. (iii) acima poderá ter fundamento, mas não se limita, às seguintes finalidades:

(i) apoio e promoção de atividades da Empresa; 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.

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

3.6.2. O consentimento de que trata o item 3.6 (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.

3.7. A Empresa 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 prestado pela Empresa em virtude de obrigação regulatória, conforme aplicável;

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

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

(iv) informações acerca do potencial compartilhamento de dados pela Empresa 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.

3.8. 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.

3.9. 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 Empresa;

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

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

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

3.11. A Autoridade Nacional de Proteção de Dados poderá determinar que a Empresa 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 Empresa sobre estas medidas, salvaguardas e mecanismos de mitigação de risco adotados.

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

CAPÍTULO IV
PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

I. ACESSO RESTRITO

4.1.1. A troca de informações entre os Colaboradores da Empresa 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 o Departamento de Compliance deve ser acionada previamente à revelação. As barreiras de informação devem ser especial atenção no compartilhamento entre Colaboradores das Empresas, tendo em vista o interesse do receptor no recebimento das informações.

4.1.2. Os Colaboradores da Empresa 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.

4.1.3. Os arquivos da Empresa são gerados e armazenados por meio do uso do serviço online denominado Microsoft *Sharepoint*.

4.1.4. 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.

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

4.1.6. O armazenamento de informações protegidas em dispositivos portáteis deve restringir-se àqueles fornecidos pela Empresa, sendo que todos os equipamentos utilizados pelos Colaboradores que possuem acesso à rede da Empresa são controlados por um sistema central do administrador da rede que restringe a utilização de dispositivos de acesso não homologados, assim como portas e periféricos de risco, tais como portas do tipo USB. Eventuais exceções devem ser previamente aprovadas pela Diretoria.

4.1.7. A outorga e cancelamento de senhas é de responsabilidade do TI, sempre mediante orientação do Diretor Compliance, a quem compete a verificação da estrutura de governança da Empresa, 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 Empresa.

4.1.8. As senhas de acesso possuem prazo de validade de 31 dias e requisitos mínimos de segurança correspondente a 9 caracteres, com histórico de 12 senhas para evitar que a mesma senha seja utilizada. As senhas que forem digitadas de maneira errônea por mais de 3 vezes são bloqueadas por 60 minutos.

4.1.9. Após um tempo máximo de inatividade, os sistemas internos e dispositivos fornecidos pela Empresa expiram, usando um protetor de tela protegido por senha que exige que a sessão somente possa ser reiniciada depois que o usuário tenha se autenticado novamente.

4.1.10. 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 Empresa deverá submeter uma solicitação de revogação de acesso imediatamente e assegurar-se de que os acessos sejam revogados.

4.1.11. O controle do acesso a arquivos confidenciais em meio físico é garantido através da segregação física de todas as Empresas, especialmente no que tange à equipe de gestão de recursos da Gama Investimentos Ltda. Adicionalmente, todas as ligações telefônicas realizadas por meio dos equipamentos disponibilizados à equipe de gestão são gravadas.

II. BACK-UP

4.2.1 Todos os documentos produzidos dentro da Empresa são objeto de backup diário em nuvem, com redundância, garantindo a segurança dos respectivos conteúdos e eventual responsabilização. Desta forma, os backups diários são realizados em nuvem disponibilizada por 2 (dois) prestadores de serviços independentes.

III. CÓPIA DE ARQUIVOS E INSTALAÇÕES

4.3.1. Todos os programas de computador utilizados pelos Colaboradores devem ter sido previamente autorizados pelo responsável pela área de informática. Downloads de qualquer natureza podem ser realizados, desde que de forma justificada.

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

4.3.3. 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 Empresa. Nestes casos, o colaborador que estiver na posse e guarda do arquivo será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

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

IV. DESCARTE DE INFORMAÇÕES

4.4.1. 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 triturados imediatamente 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 pela Empresa devem ser apagados de modo que a informação protegida que neles havia seja irrecuperável.

V. REDUNDÂNCIA

4.5.1. Todos os recursos de TI são redundantes. Em caso de pane e indisponibilidade de acesso físico ao local de trabalho e/ou ao Microsoft *Sharepoint*, a equipe-chave, previamente designada e treinada para tanto, poderá acessar as informações ao ambiente de contingência na nuvem de redundância que dá acesso a todos os recursos da Empresa.

4.5.2. No tocante ao acesso à internet, a Empresa dispõe de duas conexões banda larga ligadas simultaneamente pelo Firewall, que permite a automática comutação e a divisão

do tráfego para o serviço secundário, sempre que houver interrupção do serviço principal.

4.5.3. 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 e o 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 salvem seus arquivos.

CAPÍTULO V
SUPORTE E MONITORAMENTO

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

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

5.3. 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 Empresa também poderá monitorar toda e qualquer troca, interna ou externa, de e-mails dos Colaboradores.

5.4. 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.

5.5. 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

5.6. No caso de vazamento de informações confidenciais relacionadas aos clientes da Empresa, ou de qualquer outro Dado Pessoal ou Dado Pessoal Sensível tratado pela Empresa, ainda que oriundo de ação involuntária, o Diretor de Compliance notificará os

interessados sobre o ocorrido. Em se tratando de Dado Pessoal ou Dado Pessoal Sensível, a Autoridade Nacional de Proteção de Dados também deverá ser comunicada, além do titular do dado. Esta comunicação observará os parâmetros exigidos pela Lei Geral de Proteção de Dados.

5.7. Sem prejuízo, a Empresa 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.

5.8. Este Relatório será elaborado pelo Diretor de Compliance e será submetido à Diretoria da Empresa que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível. O referido Relatório será elaborado de forma segregada para cada Empresa afetada.

Firewall

5.9. A Empresa faz o uso da tecnologia de Firewall para proteger sua rede contra ameaças externas.

Rede Wireless

5.10. A Empresa possuí 2 (duas) redes WIFI distintas, uma para uso interno e outra para uso dos visitantes. Jamais deve ser divulgada a senha de acesso interno para os visitantes. Os visitantes devem sempre solicitar a senha de acesso para a recepcionista.

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

Testes de Segurança

5.12. São realizados os seguintes testes de segurança para monitoramento dos sistemas utilizados:

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

Sincronismo de arquivos usando DFS	Tempo real
Back Up Nuvem	Diário
Atualizações nas estações de trabalho	Mensal
Troca da senha dos usuários	Mensal

CAPÍTULO VI
IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS CIBERNÉTICOS

6.1. Abaixo são descritas as possíveis ameaças identificadas e as respectivas avaliações considerando as atividades desenvolvidas pela Empresa. Para tanto, considerou-se: (i) possíveis ameaças (internas e externas); (ii) impactos financeiros, operacionais e reputacionais; e (iii) a expectativa de que o evento de segurança (ameaça) se efetive.

6.2. Para fins de cálculo de risco, para cada impacto é estimado um nível dentro de uma escala de 1 a 5, sendo que o nível 1 significa sem impacto e o nível 5 é considerado o de impacto mais grave:

Impacto	Nível
Gravíssimo	5
Grave	4
Médio	3
Leve	2
Sem impacto	1

6.3. De maneira análoga, foi estabelecido um nível para a expectativa de ocorrência de cada ameaça utilizando a mesma escala (1 a 5), sendo o nível 1 atribuído à expectativa de ocorrência rara e o nível 5 para expectativa de ocorrência quase certa:

Expectativa de ocorrência	Nível
Quase certa	5
Alta	4
Média	3
Baixa	2
Rara	1

6.4. Desta forma, são apresentados a seguir os cálculos dos riscos, que levam em consideração: (i) a expectativa de ocorrência de cada ameaça previamente mapeada e (ii) o nível de impacto estimado em caso de ocorrência do evento de segurança:

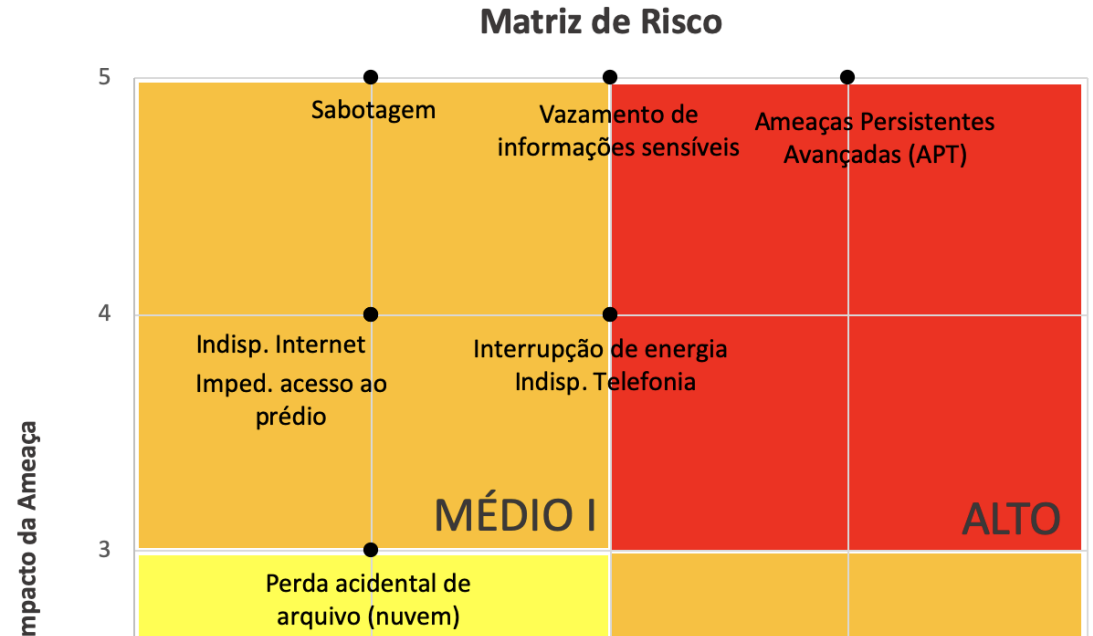
Ameaça	Expectativa do	Impacto do	Risco (ExI)

	evento (E)	evento (I)	
Falha de hardware	3	2	6
Falha de software	3	2	6
Falha de servidores em nuvem	2	2	4
Interrupção de energia	2	4	8
Ameaça Persistente Avançada (APT): phishing, malware, ransomware	4	5	20
Perda acidental de arquivos em nuvem	2	3	6
Indisponibilidade de telefonia	3	4	12
Indisponibilidade do Bloomberg	2	2	4
Indisponibilidade de Internet	2	4	8
Impedimento de acesso ao prédio	2	4	8
Vazamento de informações sensíveis (interna)	3	5	15
Sabotagem (interna)	2	5	10

6.5. O modelo de cálculo de risco considera 4 níveis de risco, por ordem de prioridade.

Risco	Nível	Faixa (ExI)
Alto	4	Maior ou igual a 15
Médio I – impacto médio/alto	3	9 a 15 (I>3)
Médio II – impacto baixo	2	9 a 15 (I<3)
Baixo	1	Menor que 9

6.6. A partir do modelo adotado, foi obtida a seguinte matriz de risco:



6.7. Ademais, a matriz de risco acima levou em consideração que, tendo em vista que a atividade de gestão profissional de recursos de terceiros desempenhada pela Gama, são essenciais todos os recursos tecnológicos necessários ao **processo de análise, investimento e desinvestimento, tais como:** (i) disponibilização das 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:

- *SMA – sistema do administrador dos fundos;*
- *Sistema BlueTis*
- *Connect – Sistema para gestão de contas no exterior*
- *Bancos – Sistema para gestão de contas correntes*
- *CVM e Anbima – Sites regulatórios*
- *Prefeituras de São Paulo e Porto Alegre – Para emissão de NF e NFTS*

CAPÍTULO VII
AÇÕES DE PROTEÇÃO E PREVENÇÃO AOS RISCOS CIBERNÉTICOS

7.1. 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 as ameaças identificadas se concretizem.

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

7.3. 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 barreiras da informação com relação a outras atividades desempenhadas pela Empresa ou empresas do mesmo grupo econômico.

7.4. Os eventos de login e alteração de senhas são rastreáveis e auditáveis, sendo qualquer inconsistência 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.

7.5. São adotadas as seguintes medidas preventivas para cada ameaça identificada:

Ameaça Interna	**Ação de Proteção/Prevenção**
Falha no backup	*Redundância de backup em outra nuvem*
Acesso a conteúdo prejudicial (internet)	*Políticas de acesso restritivas*
Vazamento de informação	*Firewall bloqueia acesso a sites de compartilhamento de arquivos e drives virtuais, sendo liberado, com a aprovação do diretor de Compliance.*
Sabotagem	*N/A*

Ameaça Externa	**Ação de Proteção/Prevenção**
APT	*Políticas restritivas de acesso aos sistemas da Empresa, criptografia forte e autenticação em várias pontas de acesso*
Phishing	*Filtro de conteúdo de e-mail, antivírus em tempo real*
Malware	*Anti-vírus de firewall em tempo real, antivírus no endpoint saneando em tempo real, políticas de execução de aplicativos restrita para administradores da área de tecnologia*
Ransomware	*Antivírus em tempo real, políticas de execução de aplicativos restrita para administradores da área de tecnologia*

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

7.7. 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 VIII
MECANISMOS DE SUPERVISÃO DA SEGURANÇA CIBERNÉTICA

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

Rotina	**Periodicidade**
backup	*Diário*
Teste de restauração de dados	*Diário*
Análise de Logs e trilhas de auditoria	*Os logs são armazenados e analisados de forma manual quando necessário.*

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

8.3. Sempre que houver alteração relevante na estrutura tecnológica da Empresa serão realizadas análises de vulnerabilidade.

CAPÍTULO IX
RESPOSTAS A INCIDENTES CIBERNÉTICOS

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

Ameaça Interna	**Risco/Severidade**	**Plano de Ação**
Falha de Hardware Endpoint	*Média II*	*Reportar ao TI, realizar testes relacionados ao hardware, e providenciar o reparo ou a troca do equipamento*
Falha de Software Endpoint	*Média II*	*Reportar ao TI, testar o software e verificar as soluções conhecidas para o*

		problema, em caso de falha entrar em contato com fabricante do software para conseguir mais informações sobre o problema
Falha de Hardware/Software da nuvem	*Baixa*	*Analisar os sintomas do defeito do Software ou Hardware e providenciar o reparo/ troca do mesmo.*
Interrupção do fornecimento de energia	*Média I*	*Informar ao TI e verificar a causa da queda, se necessário ir fisicamente desligar o ambiente tecnológico da Empresa de maneira correta*
Infecção de Malware	*Alta*	*Informar ao TI, Aguardar a análise do tipo de malware e a possibilidade de desinfecção do mesmo, caso não seja sucedida aguardar o plano dos responsáveis de TI.*
Exclusão acidental de arquivo da nuvem	*Baixa*	*Informar ao TI, e aguardar o "restore" do arquivo.*
Indisponibilidade do serviço de telefonia	*Média I*	*Informar ao TI e a prestadora de Telefonia e aguardar a investigação do porquê da indisponibilidade*

Ameaça Externa	**Risco/Severidade**	**Plano de Ação**
Indisponibilidade do serviço Bloomberg	*Baixa*	*Informar ao TI, aguardar a troca para o serviço de contingência, em seguida identificar o motivo da indisponibilidade*
Indisponibilidade do serviço de internet	*Média I*	*Informar ao TI, aguardar a troca para o link de contingência, em seguida identificar o motivo da indisponibilidade*
Impossibilidade de acessar a matriz fisicamente	*Baixa*	*Analisar o motivo da falta de acesso físico ao ambiente e se for possível acessar remotamente através do Microsoft Sharepoint*

9.2. Compete ao Departamento de Compliance a comunicação da contingência aos demais Colaboradores da Empresa, 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.

9.3. Cabe, ainda, ao Departamento de Compliance 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 executadas normalmente, sendo que os referidos relatórios serão elaborados de forma segregada para cada Empresa. Tais relatórios deverão ser submetidos à Diretoria da Empresa que promoverá as iniciativas cabíveis para o retorno à normalidade com a maior brevidade possível.

9.4. Após o retorno à normalidade, na tentativa de evitar incidentes da mesma qualidade, a Empresa estudará procedimentos preventivos a serem implementados e incluídos neste plano de continuidade de negócios.

CAPÍTULO X
PROGRAMA DE TREINAMENTO

10.1. A Empresa conta com um programa de treinamento dos Colaboradores que tenham acesso a informações relevantes sobre a Empresa, seus negócios ou clientes, na forma descrita no Manual 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.

10.2. Os 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 Empresa.

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

CAPÍTULO XI
DISPOSIÇÕES GERAIS E *ENFORCEMENT*

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

11.2 A presente Política prevalece sobre quaisquer entendimentos orais ou escritos anteriores, obrigando os Colaboradores da Empresa aos seus termos e condições.

11.3. A título de *enforcement*, vale notar que a não observância dos dispositivos da presente Política resultará em advertência, suspensão, demissão ou exclusão por justa causa, conforme a gravidade e a reincidência na violação, sem prejuízo das penalidades civis e criminais.

Histórico de Versões

Versão	Mês/Ano	Itens Revisados:
1ª	02/2019	Política de Segurança da Informação extraída do Código de Ética. Inclusão dos procedimentos de cibersegurança.
2ª	01/2020	Ajustes no texto com base no modelo de risco de TI adotado (que utiliza adequadamente o conceito de ameaça, impacto e risco).
3ª	01/2021	Inclusão do Capítulo II – Proteção de Dados Pessoais e ajustes na redação.
4ª	07/2022	Revisão geral da Política
5ª	05/2023	Ampliação da abrangência da Política.