POLÍTICA DE SEGURANÇA DE INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

CONTROLE DE VERSÕES

VERSÃO	DATA	ELABORADOR/MODIFICADO POR	DESCRIÇÃO
1ª	01/07/2016	Pedro Romeiro / Celso Casaro	Versão Original
2ª	02/01/2019	Pedro Romeiro / Celso Casaro	1ª Alteração
3ª	15/01/2020	Pedro Romeiro / Celso Casaro	2ª Alteração
4ª	14/09/2020	Pedro Romeiro / Celso Casaro	3ª Alteração
5ª	17/12/2021	Pedro Romeiro / Celso Casaro	4ª Alteração
6ª	02/04/2024	Pedro Romeiro / Celso Casaro	5ª Alteração

Sumário

1. Do Objetivo

Esta Política de Segurança de Informação e Segurança Cibernética tem por objetivo estabelecer os fundamentos e diretrizes, a serem obrigatoriamente observados pelo grupo Carpa Family Office (a "Carpa Family Office") e todos os seus colaboradores, de segurança de informação e cibernética que assegurem a confidencialidade, a integridade e a disponibilidade de dados e sistemas de informação, observando a natureza das operações, a complexidade dos produtos, dos serviços, das atividades e processos, bem como o porte, perfil de risco, modelo de negócio e a sensibilidade dos dados e das informações sob responsabilidade da instituição (a "Política" e a "Segurança de Informação e Cibernética").

A presente Política também apresenta procedimentos que visam:

a) Estabelecer o conceito de que as informações são ativos de extrema importância para a organização;
b) Envolver formalmente os sócios, diretores, colaboradores e terceiros contratados pela Carpa Family Office (os "Colaboradores") sobre a salvaguarda dos recursos da informação, definindo o conceito de irrevogabilidade;
c) Conscientizar todos os Colaboradores sobre os riscos existentes e a importância da Segurança da Informação;
d) Apresentar normas e condutas para o manuseio, controle e proteção das informações;
e) Estabelecer padrões para a manutenção e cumprimento da Segurança da Informação;
f) Fornecer aos Colaboradores orientações, descrevendo suas responsabilidades pessoais, necessidade de privacidade e sigilo, e informando, ainda, quais os procedimentos adequados e/ou indevidos do ponto de vista da Segurança da Informação; e
g) Agregar à organização um diferencial competitivo, a fim de apresentar a seus clientes e parceiros o compromisso da Carpa Family Office em garantir a segurança de suas informações.

2. Abrangência

As disposições definidas nesta Política devem ser aplicadas a todos os Colaboradores que possuam acesso às dependências e/ou que tenham acesso a qualquer tipo de ativo de informação que pertença, ou que estejam sob a responsabilidade da Carpa Family Office.

3. Ativos de Informação

A Carpa Family Office considera como ativos de informação todas as informações, disponíveis em qualquer meio, utilizadas ou manipuladas nas operações da empresa, bem como todos os sistemas, equipamentos e instalações onde estas informações são manuseadas ou armazenadas.

As informações podem ser apresentadas nas mais distintas formas escritas, faladas, transmitidas, digitadas, armazenadas ou processadas em qualquer equipamento, papel, telefone, programa de computador, base de dados ou outro meio existente. Seja qual for o estado ou o meio do qual a informação seja apresentada ou compartilhada, ela deverá estar sempre protegida adequadamente, de acordo com as normas definidas neste documento.

Para que não haja dúvidas, a Carpa Family Office define como ativos de informação os seguintes itens:

a) As informações criadas, processadas, acessadas, manuseadas ou armazenadas em qualquer meio ou sistema de informação da Carpa Family Office;
b) Os computadores, equipamentos, *softwares*, banco de dados, redes de comunicações e serviços de tecnologia utilizados pela empresa em suas operações, ou qualquer outro recurso, informático ou não, que seja utilizado nas atividades da empresa onde haja manipulação ou armazenamento de informações;
c) As instalações em que estão localizados os equipamentos, sistemas, documentos ou informações da Carpa Family Office;
d) Processos e controles internos que sejam parte da rotina das áreas de negócio da Carpa Family Office; e
e) Governança da gestão de risco quanto às ameaças e planos de ação, de contingência e de continuidade de negócios.

4. Comprometimento da Diretoria

Atingir um padrão eficiente e consistente de boas práticas para a Segurança da Informação e Cibernética em toda a empresa exige direcionamento claro e comprometimento por parte da alta direção. Desta forma, a Carpa Family Office se compromete a atingir altos padrões de governança corporativa, tratar Segurança da Informação e Cibernética como elemento vital ao negócio, criar um ambiente positivo de segurança, e demonstrar a terceiros que a empresa trata a Segurança da Informação e Cibernética de forma profissional e compatível com sua estrutura e operações

5. Conceito de Segurança Cibernética

Enquanto a segurança de informação engloba políticas e práticas visando a proteção de informações confidenciais, a segurança cibernética em si constitui-se da preservação das propriedades da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e o compartilhamento da informação de forma controlada, bem como do monitoramento e tratamento de incidentes provenientes de ataques cibernéticos.

No que se refere especificamente à segurança cibernética, a Carpa Family Office identificou as seguintes principais ameaças, nos termos inclusive do Guia de Cibersegurança da ANBIMA:

- *Malware – softwares* desenvolvidos para corromper computadores e redes (tais como: Vírus, Cavalo de Troia, *Spyware* e *Ransomware*);
- Engenharia social – métodos de manipulação para obter informações confidenciais (*Pharming*, *Phishing*, *Vishing*, *Smishing*, e Acesso Pessoal);
- Ataques de DDoS (*distributed denial of services*) e *botnets*: ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; e
- Invasões (*advanced persistent threats*): ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Com base na informação acima, a Carpa Family Office avalia e define o plano estratégico de prevenção e acompanhamento para a mitigação ou eliminação do risco, assim como as eventuais modificações necessárias e o plano de retomada das atividades normais e reestabelecimento da segurança devida.

6. Classificação da Informação

Observadas as Diretrizes de Comportamento Seguro, dispostas no Capítulo 12 abaixo, todas as informações devem ter classificação de segurança, de maneira a serem adequadamente protegidas quanto ao seu acesso e uso, sendo que, para aquelas consideradas de alta criticidade, são necessárias medidas especiais de tratamento. A classificação das informações deverá seguir a seguinte ordem:

a) Informações públicas – são aquelas que não necessitam de sigilo, de livre acesso aos Colaboradores. São informações que se forem divulgadas fora da organização, não terão impactos para a organização. São exemplos dessas informações:

- Brochuras / *folders* sobre a Carpa Family Office;
- Campanha de *marketing* finalizada;
- Política regulatórias disponíveis ao público em geral em seu site;
- Informações geradas para consumo público; ou
- Informações financeiras publicadas em um jornal ou similares.

b) Informações internas – são aquelas cujo acesso externo deve ser evitado. Apenas funcionários devem possuir acesso a essas informações e só devem ser utilizadas para atender às necessidades da Carpa Family Office. São informações que, se forem divulgadas fora da organização, terão impacto indesejável para a organização, embora as consequências não sejam críticas. São exemplos dessas informações:

- Documentos que descrevem a rotina da Carpa Family Office;
- Memorandos e comunicados internos;
- Políticas corporativas internas, padrões e procedimentos;
- Agendas de telefones e ramais internos; ou
- Benefícios oferecidos pela empresa.

c) Informações restritas – São as informações internas de alto valor e sensibilidade que podem trazer prejuízo ao grupo Carpa Family Office em caso de divulgação e apenas Colaboradores necessários podem ter acesso. São exemplos dessas informações:

- Planos de negócios;
- Propriedade intelectual; e
- Pesquisas em andamento.

d) Informações confidenciais – São as informações confidenciais, reservadas ou privilegiadas que devem ser confidenciais dentro da organização e protegidas de acessos externos, e apenas Colaboradores necessários poderão ter acesso. Se alguma dessas informações for acessada por indivíduos não autorizados, as operações da organização poderão ser comprometidas, causando perdas financeiras e de produtividade. Informações confidenciais não podem ser transportadas ou transmitidas sem as devidas autorizações e proteções. A integridade dessas informações é vital. A seguir, são apresentados exemplos dessas informações:

- Detalhes técnicos sobre produtos em desenvolvimento, bem como informações financeiras ou relacionadas a estratégias de investimento e desinvestimento, ou comerciais; incluindo saldos, extratos e posições de clientes dos fundos de investimento;
- Know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador;
- Contratos entre clientes e fornecedores;
- Informações de colaboradores, fornecedores e clientes, bem como relação de contrapartes comerciais e prestadores de serviços;
- Estratégia de mercado ou de qualquer natureza relativas às atividades da Carpa Family Office e a seus sócios ou clientes, incluindo alterações societárias (fusões, cisões e incorporações), informações sobre compra e venda de empresas, títulos ou valores mobiliários, inclusive ofertas iniciais de ações (IPO), projetos e qualquer outro fato que seja de conhecimento em decorrência do âmbito de atuação da Carpa Family Office e que ainda não foi devidamente levado à público;
- Negócios realizados e que ainda não foram publicados, bem como operações estruturadas, demais operações e seus respectivos valores analisadas ou realizadas pelos fundos de investimento;
- Posições compradas ou vendidas e que ainda não tenham sido divulgadas publicamente;
- Relatórios, análises e opiniões sobre ativos financeiros;

- Dados a respeito de resultados financeiros antes da publicação dos balanços e balancetes da Carpa Family Office e dos fundos cujas carteiras sejam geridas pela Carpa Family Office;
- Endereços de IPs internos;
- Nome de servidores;
- Chaves de acesso (senhas);
- Sistemas;
- Códigos fontes de sistemas;
- Papéis de trabalho (Fiscal, Auditoria, Operacional, Risco, entre outros); e
- Outras informações obtidas junto aos Colaboradores da Carpa Family Office ou, ainda, junto a seus representantes, consultores, assessores, clientes, fornecedores e prestadores de serviços em geral.

Nível de Classificação	**Valor**	**Sensibilidade**	**Acesso**	**Risco de divulgação**	**Sanções por divulgação**
Pública	Baixo	Baixa	Livre	Baixo	Nenhuma
Interna	Médio	Média	Colaboradores com necessidade de acesso	Médio	Disciplinares
Restrita	Alto	Alta	Colaboradores autorizados com aprovação formal	Alto	Disciplinares e legais
Confidencial	Extremamente Alto	Extremamente Alta	Acesso extremamente restrito com aprovação formal	Extremamente alto	Disciplinares, legais e criminais

Nenhuma informação da Carpa Family Office classificada como confidencial pode ou deve ser discutida em locais inapropriados, como lugares públicos ou fechados, na presença de terceiros ou pessoas não diretamente relacionadas ao assunto, ou diante daqueles sem autorização para conhecimento dessas informações.

Qualquer informação sobre a Carpa Family Office, ou de qualquer natureza relativa às atividades da Carpa Family Office e aos sócios e clientes, obtida em decorrência do desempenho das atividades normais do Colaborador na Carpa Family Office, só poderá ser fornecida ao público, mídia ou a demais

órgãos caso autorizado pelo *Compliance* da Carpa Family Office, apontado nos termos do Código de Ética, Regras, Procedimentos e Controles Internos da Carpa Family Office.

Conforme o descrito acima, a informação alcançada em função da atividade profissional desempenhada por cada Colaborador na Carpa Family Office não pode ser transmitida de forma alguma a terceiros não Colaboradores ou a Colaboradores não autorizados.

7. Acesso à Informação e Uso de Equipamentos

- Acesso Escalonado e Diferenciado do Sistema

Os acessos às informações (dados) e aos ambientes lógicos (sistemas) devem ser controlados, de forma a garantir o efetivo acesso apenas de pessoas autorizadas, sendo certo que tal restrição/segregação será feita em relação a: (i) área/atividade, (iii) cargo/nível hierárquico e (iii) equipe.

A rede de computadores da Carpa Family Office permite a criação de Colaboradores com níveis de permissão diferentes, por meio de uma segregação lógica nos servidores que garantem que cada departamento conte com uma área de armazenamento de dados distinta no servidor com controle de acesso por Colaborador.

Os Colaboradores autorizados possuem chaves de acessos (senhas) autorizando seu efetivo acesso aos recursos da Carpa Family Office, de acordo com suas responsabilidades. Não será permitido que o Colaborador execute transações incompatíveis com sua função.

Em casos de transferência entre áreas, o gestor da área para qual o Colaborador for transferido deverá solicitar os acessos e o gestor da área cedente deverá solicitar o cancelamento de todos os acessos relativos às suas respectivas áreas.

Os acessos aos recursos críticos são monitorados e registrados, esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

Os registros são protegidos e armazenados de acordo com a sua classificação e mantidos sob custódia do Departamento de Tecnologia e Segurança da Informação. A Carpa Family Office dispõe, como padrão de segurança lógica, os seguintes itens:

a) *Firewall* com monitoramento para acesso à *Internet*;
b) Sistema de detecção de intrusão (IDS);
c) *Login* único com fator adicional de autenticação;
d) Acesso remoto através de rede privada virtual (VPN);
e) Utilização de identificadores de Colaborador (ID de Colaborador) individualizados, de forma a assegurar a responsabilidade de cada Colaborador por suas ações;
f) Registro de segurança para sistemas e dados críticos; e
g) Metodologia de Controle de Acesso para cada sistema.

Cada Colaborador terá à disposição uma pasta própria de acesso exclusivo para digitalizar os respectivos arquivos, garantindo acesso exclusivo do Colaborador aos documentos de sua responsabilidade. Em caso de desligamento do Colaborador, todos os arquivos salvos no respectivo diretório pessoal serão transmitidos à pasta do seu superior direto, a fim de evitar a perda de informações.

- <u>Uso de Equipamentos e Sistemas</u>

Todos os Colaboradores são responsáveis individualmente pelos equipamentos que utilizam ou gerenciam e devem estar cientes do seu comprometimento pelo uso adequado deles.

A utilização dos ativos e sistemas da Carpa Family Office, incluindo computadores, telefones, internet, e-mail e demais aparelhos se destina prioritariamente a fins profissionais. O uso indiscriminado destes para fins pessoais deve ser evitado e nunca deve ser prioridade em relação a qualquer utilização profissional.

Como já mencionado anteriormente, todo Colaborador deve ser cuidadoso na utilização do seu próprio equipamento e sistemas e zelar pela boa utilização dos demais. Caso algum Colaborador identifique a má conservação, uso indevido ou inadequado de qualquer ativo ou sistemas deve comunicar o fato a qualquer dos membros do *Compliance*.

Os Colaboradores devem se abster de utilizar *pen-drives*, disquetes, fitas, discos ou quaisquer outros meios que não tenham por finalidade a utilização exclusiva para o desempenho de sua atividade na Carpa Family Office.

É proibida a conexão de equipamentos na rede da Carpa Family Office que não estejam previamente autorizados pela área de Departamento de Tecnologia e Segurança da Informação e pelo *Compliance*.

- Senha e Login

A senha e login para acesso aos dados contidos em todos os computadores, bem como nos e-mails que também possam ser acessados via webmail, devem ser conhecidas pelo respectivo usuário do computador e são pessoais e intransferíveis, não devendo ser divulgadas para quaisquer terceiros.

Para segurança dos perfis de acesso dos Colaboradores, as senhas de acesso dos Colaboradores são parametrizadas conforme as regras determinadas pelo *Compliance*, para implementação nos perfis de acesso dos Colaboradores, sendo certo que tais senhas são alteradas a cada 42 dias.

Dessa forma, o Colaborador pode ser responsabilizado inclusive caso disponibilize a terceiros a senha e *login* acima referidos, para quaisquer fins.

- Uso de Equipamentos e Sistemas

Cada Colaborador é responsável por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos que estão sob sua responsabilidade.

Para tanto, cada Colaborador que receber equipamentos da Carpa Family Office para uso fora do escritório deverá assinar um contrato de comodato nos termos do modelo anexo a esta Política.

- Ligações Telefônicas e Aplicativos de Mensagens Instantâneas

Todas as comunicações telefônicas da Carpa Family Office - hoje nas áreas operacionais, 100% via Microsoft Teams, são gravadas de forma contínua. Assim, a Carpa Family Office poderá, quando entender necessário e a seu exclusivo critério, interceptar e escutar, bem como realizar o monitoramento, por amostragem, das ligações dos seus Colaboradores realizadas ou recebidas por meio das linhas disponibilizadas pela Carpa Family Office para a atividade profissional de cada Colaborador, especialmente, mas não se limitando, às ligações da equipe de atendimento e da mesa de operação da Carpa Family Office.

Clientes que contratam os Serviços Familiares da Carpa Family Office tem a opção do uso do whatsapp business ou aplicativo que o substituir, para o envio de solicitações de pagamento ou transferências, de documentos, de orientação de voto ou qualquer outra comunicação com a Carpa Family Office a despeito de sua vulnerabilidade.

Para tanto, o cliente assina um termo específico de responsabilidade e de isenção de responsabilidade da Carpa Family Office por eventuais solicitações realizadas por criminosos ou terceiros que tenham tido acesso ao celular ou aparelho eletrônico que o cliente ou seus representantes se utilizam para o envio de mensagens pelo whatsapp e similares e venham a se passar por ele(s).

No mais, clientes em geral se comunicam por whatsapp para os mais diversos assuntos com a Carpa Family Office e, dentro do possível, conforme determinação do cliente, a orientação geral é não enviar documentos confidenciais ou restritos por tais aplicativos.

- <u>Acesso Remoto</u>

A Carpa Family Office permite o acesso remoto por todos os Colaboradores desde que seus laptops tenham instalados os requisitos de segurança cibernética da Carpa Family Office,

Ademais, os Colaboradores são instruídos a (i) manter softwares de proteção contra malware/antivírus nos dispositivos remotos, (ii) relatar ao *Compliance* e ao Departamento de Tecnologia e Segurança da Informação qualquer violação ou ameaça de segurança cibernética ou outro incidente que possa afetar informações da Carpa Family Office durante o trabalho remoto, e (iii) não armazenar informações confidenciais ou sensíveis em dispositivos pessoais.

Os acessos físicos devem ser controlados e orientados, de forma a garantir que apenas pessoas autorizadas possuam o efetivo acesso às instalações e equipamentos que pertençam e/ou que sejam utilizados pela Carpa Family Office. Os recursos de tecnologia da informação e comunicação que estiverem contidos e/ou que forem utilizados pela Carpa Family Office também devem ser abrangidos, sendo o seu acesso restrito a pessoas devidamente autorizadas.

O acesso ao prédio e determinadas salas será constantemente monitorado em função de ser realizado por meio de cartão de acesso ou reconhecimento facial, de acordo com cada perfil criado e de acordo com as responsabilidades de cada Colaborador, evitando-se acessos indevidos de Colaboradores a áreas não autorizadas.

Para acesso aos equipamentos informáticos, os Colaboradores possuem chaves de acessos (senhas) que também são criadas com perfis distintos, permitindo ao Colaborador acessar os equipamentos de acordo com suas responsabilidades.

As instalações da Carpa Family Office possuem sistema de vigilância monitorado em tempo real. Este sistema também realiza a gravação dos eventos ocorridos, permitindo uma análise posterior detalhada.

Visitantes das instalações da Carpa Family Office devem ser supervisionados. Esses indivíduos devem ter acesso apenas às áreas específicas, com propósitos autorizados e sempre acompanhados por pessoas autorizadas a acessar esses ambientes.

Perda da chave de acesso deve ser imediatamente comunicada ao Departamento de Tecnologia e Segurança da Informação e ao *Compliance*, que tomará as medidas apropriadas para prevenir acessos não autorizados.

Para a sala de servidores, denominada sala fria, adota-se como padrão de segurança os seguintes itens:

a) Piso elevado com altura mínima de 10 cm;
b) Refrigeração com redundância;
c) Acesso restrito por leitura facial de Colaboradores;

d) Nobreak; e

e) Sistema de detecção e combate a incêndio.

8. Metodologia de Backup, Firewall, Software e Varreduras

Todas as informações do servidor da Carpa Family Office, do banco de dados dos clientes e os modelos dos analistas são enviados para o servidor em nossa nuvem do Azure. Nesse servidor, as informações são segregadas por área, sendo armazenadas com *backup* redundante.

A guarda de dados é efetuada de acordo com uma política de backup configurada em nossos servidores em nuvem, que mantém uma cópia dos dados com a seguinte configuração, backups diários por 90 dias, semanais por 52 semanas, mensais por 60 meses e anual por 10 anos.

Para servidores locais, com máquinas virtuais configuradas para executar funções de redundância de alguns recursos da nuvem, o *backup* é efetuado através das mesmas políticas dos servidores do Azure.

A rotina de *backup* é padronizada, com estrutura definida considerando os conceitos de performance, disponibilidade e compatibilidade. As informações da Carpa Family Office são atualmente objeto de backup diário.

Os dados de backups ficam em um *data center* da Microsoft localizado no sul do Brasil e seguem as políticas de redundância do Azure.
Ademais, a Carpa Family Office utiliza um hardware de firewall projetado para evitar e detectar conexões não autorizadas e incursões maliciosas. O Diretor de *Compliance* junto do Diretor de Tecnologia e Segurança da Informação é o responsável por determinar o uso apropriado de firewalls (por exemplo, perímetro da rede).

A Carpa Family Office mantém proteção atualizada contra *malware* nos seus dispositivos e software antivírus projetado para detectar, evitar e, quando possível, limpar programas conhecidos que afetem

de forma maliciosa os sistemas da empresa (por exemplo, vírus, *worms*, *spyware*). São conduzidas varreduras semanais para detectar e limpar qualquer programa que venha a obter acesso a um dispositivo na rede da Carpa Family Office.

A Carpa Family Office utiliza um plano de manutenção projetado para guardar os seus dispositivos e softwares contra vulnerabilidades com o uso de varreduras e patches. O Diretor de Tecnologia e Segurança da Informação é o responsável por patches regulares nos sistemas da Carpa Family Office.

- Monitoramento de Tráfego de Dados – *Data Loss Prevention*

O processo de *Data Loss Prevention* – DLP tem como objetivo monitorar o tráfego de dados em e-mails, arquivos, mensagens instantâneas e outras plataformas, identificando e bloqueando tentativas de transferência não autorizada de informações confidenciais.

Criptografia de dados: O DLP pode criptografar dados confidenciais antes de sua transferência, garantindo que apenas os destinatários autorizados possam acessá-los.

Controle de dispositivos: O DLP pode controlar o uso de dispositivos removíveis e periféricos, impedindo a transferência não autorizada de dados para dispositivos externos.

Detecção de conteúdo sensível: O DLP utiliza técnicas avançadas para detectar a presença de conteúdo sensível em documentos, e-mails e outros arquivos, alertando os usuários sobre possíveis violações.

9. Fatores Críticos de Sucesso

O Colaborador deve ter consciência de que a informação é um bem de extrema importância para a Carpa Family Office e que o uso indevido dos ativos de informação pode causar sérios danos à organização. A proteção dos bens de informação da organização não é somente de responsabilidade dos departamentos de Tecnologia e Segurança da Informação, e de *Compliance*, mas sim de todos os Colaboradores, sendo de responsabilidade de cada um o cumprimento do disposto nesta Política.

No âmbito empresarial, só é permitido o uso de recursos tecnológicos disponibilizados pela Carpa Family Office, ou devidamente autorizados pelo Departamento de Tecnologia e Segurança da Informação. Estes recursos devem ser utilizados de forma a garantir que os requisitos de segurança sejam atendidos. Devem ser realizadas apenas atividades lícitas, éticas e que atendam aos negócios da Organização.

Todos os Colaboradores, ao tomarem conhecimento de qualquer incidente referente à segurança da informação, devem notificar o fato, imediatamente, ao Departamento de Tecnologia e Segurança da Informação, e ao *Compliance*, via *e-mail*.

10. Do Departamento de Tecnologia e Segurança da Informação

O Departamento de Tecnologia e Segurança da Informação é responsável por divulgar e estabelecer procedimentos de segurança, assim como se reunir periodicamente, ou a qualquer momento, conforme requerido pelas circunstâncias, com o objetivo de manter a segurança a níveis aceitáveis em todas as áreas da organização.

O Departamento de Tecnologia e Segurança da Informação fica incumbido de apoiar, informar, monitorar e garantir o devido cumprimento de todas as normas apresentadas nos documentos que compõem esta Política.

O monitoramento sobre o cumprimento das normas e identificação de suspeitos dar-se-á da seguinte forma:

a) Deverá monitorar, quando solicitado pelo Compliance, o acesso dos Colaboradores a sites, blogs, *fotologs*, *webmails*, entre outros, bem como os e-mails enviados e recebidos, sem prejuízo do monitoramento por termos específicos utilizados através do sistema especializado;

b) Deverá verificar, por amostragem, as informações de acesso ao espaço do escritório, a desktops, pastas e sistemas, de forma a avaliar sua aderência às regras de restrição de acesso e escalonamento;

c) Deverá identificar os Colaboradores que violarem qualquer item das normas de segurança com base nas verificações descritas acima;

d) Havendo transgressão, esses infratores serão notificados, via *e-mail*, do descumprimento das normas estabelecidas neste documento, sendo que uma cópia da notificação será enviada para o Superior direto e Compliance. Caso na infração cometida esteja caracterizado qualquer tipo de crime (acesso a *sites* de pedofilia, racismo etc.), aplicar-se-á sanções especiais.

O Departamento de Tecnologia e Segurança da Informação também exercerá as seguintes atividades para o procedimento de resposta aos descumprimentos pelos Colaboradores que tenham sido identificados:

a) Avaliar o tipo de incidente ocorrido (por exemplo, infecção de malware, intrusão da rede, furto de identidade), as informações acessadas e a medida da respectiva perda;
b) Determinação dos papéis e responsabilidades do pessoal apropriado;
c) Avaliação da necessidade de recuperação e/ou restauração de eventuais serviços que tenham sido prejudicados;
d) Avaliação da necessidade de notificação de todas as partes internas e externas apropriadas (por exemplo, clientes ou investidores afetados, segurança pública);
e) Avaliação da necessidade de publicação do fato ao mercado, nos termos da regulamentação vigente (por exemplo: em sendo informações confidenciais de fundo de investimento sob gestão da Carpa Family Office, a fim de garantir a ampla disseminação e tratamento equânime da Informação Confidencial);
f) Determinação do responsável (ou seja, a Carpa Family Office ou o cliente ou investidor afetado) que arcará com as perdas decorrentes do incidente. A definição ficará a cargo do *Compliance*, após a condução de investigação e uma avaliação completa das circunstâncias do incidente;
g) Propor iniciativas e projetos referentes à melhoria, ao aprimoramento e aos ajustes da Segurança da Informação;

h) Elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão; e

i) Acompanhar o andamento dos principais projetos e iniciativas relacionados à Segurança da Informação.

11. Diretrizes de Comportamento Seguro

Devem ser seguidos alguns comportamentos essenciais para garantir o devido sigilo e segurança dos ativos de informação sob gestão da empresa, conforme a seguir:

a) Não fale sobre assuntos sensíveis ou sigilosos com terceiros ou em locais públicos;

b) Não diga sua senha para ninguém. Caso sejam solicitadas, por qualquer indivíduo, informações sobre suas senhas, o Colaborador deve comunicar imediatamente o Compliance;

c) Não digite suas senhas ou *login* em máquinas de terceiros, especialmente fora da empresa;

d) Somente aceite ajuda técnica de um membro de nossa equipe técnica;

e) Nunca execute procedimentos técnicos, cujas instruções tenham sido enviadas por *e-mail* ou telefone. Em caso de extrema necessidade, confirme devidamente a identificação do solicitante;

f) Nunca passe informações detalhadas sobre a organização por telefone ou *e-mail*, principalmente se a conversa for realizada com terceiros ou sem a devida identificação;

g) Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos e, de acordo com sua classificação, destruídos, observado o disposto abaixo; e

h) Caso o Colaborador suspeite de qualquer situação ou se depare com qualquer atitude que venha a discordar das normas apresentadas neste documento, deve comunicar imediatamente o *Compliance*.

Em referência à impressão e descarte de documentos, para os fins do disposto no item "g" acima, é terminantemente proibido que os Colaboradores façam cópias ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da Carpa Family Office e circulem em ambientes externos à Carpa Family Office com estes arquivos, uma vez que tais arquivos contenham informações que são consideradas informações confidenciais.

A proibição acima referida não se aplica quando as cópias ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da Carpa Family Office e de seus clientes. Nestes casos, o Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

Ainda, qualquer impressão de documentos deve ser imediatamente retirada da máquina impressora, pois podem conter informações restritas e confidenciais, mesmo no ambiente interno da Carpa Family Office.

O descarte de documentos físicos que contenham informações confidenciais ou de suas cópias deverá ser realizado imediatamente após seu uso, de maneira a evitar sua recuperação.

O acesso à *internet* somente deve ser realizado para finalidades relacionadas aos interesses e assuntos profissionais da Carpa Family Office. O acesso à *internet* para atividades pessoais deverá ser realizado com bom senso, preferencialmente, fora do horário de trabalho e será monitorado pela Carpa Family Office, nos termos da Cláusula 13ª abaixo.

É proibida a utilização de *softwares* de compartilhamento ou troca de arquivos pela *internet* exceto aqueles fornecidos pela Carpa Family Office.

É proibido o acesso a *sites* cujo conteúdo seja inapropriado, como pornografia, atividades criminais ou não éticas e raciais.

12. Diretrizes para Utilização de E-Mail e Mensagens Instantâneas

Os serviços de *e-mail* e sistemas de mensagens instantâneas da Carpa Family Office estão disponíveis apenas para enviar e receber mensagens eletrônicas que se atenham aos negócios e interesses da empresa. Sendo assim, é de extrema importância que se estabeleça um conjunto de regras que possibilitem a utilização adequada desse importante recurso tecnológico.

Será de responsabilidade de cada Colaborador, zelar pelo fiel cumprimento das normas estabelecidas no presente documento.

Todos os Colaboradores que possuírem acessos e/ou utilizarem os serviços de correio eletrônico ou sistemas de mensagens instantâneas deverá fazê-lo no restrito interesse da Carpa Family Office, sendo o uso para fins pessoais ou particulares realizados com bom senso, respeitando-se o Código de Ética, Regras, Procedimentos e Controles Internos, e esta Política.

É proibido utilizar o serviço de *e-mail* corporativo para enviar e/ou receber materiais ilícitos, tais como: mp3, vídeos, programas e afins, independente destes arquivos estarem ou não compactados;

Por se tratar de um meio de comunicação para informações sensíveis, tanto o correio eletrônico quantos os sistemas de mensagens instantâneas (contas corporativas criadas para a organização) devem ser configurados apenas em equipamentos corporativos ou equipamentos portáteis autorizados pela *Compliance* e pelo Departamento de Tecnologia e Segurança da Informação.

Cada Colaborador tem direito a apenas uma única conta corporativa de correio eletrônico ou mensagens instantâneas.

O Colaborador é pessoalmente responsável por todas as atividades realizadas por intermédio de sua conta corporativa de *e-mail* e/ou mensagens instantâneas.

Mediante necessidade específica, poderá ser dado a um Colaborador o direito de acessar a conta de correio eletrônico ou de mensagens instantâneas de outro Colaborador. A autorização deste procedimento deve ser solicitada mediante a abertura de chamado via *e-mail*, e será submetido à aprovação do *Compliance*. Após aprovação, o referido procedimento pode ser realizado pelos administradores dos serviços.

É de responsabilidade do Colaborador a manutenção da caixa de *e-mail* de sua propriedade, devendo fazer a exclusão ou o arquivamento das mensagens a fim de manter espaço livre.

A conta de *e-mail* possui limite de armazenamento no servidor de *e-mail*, chegando ao limite de armazenamento, o Colaborador será notificado e deverá providenciar sua manutenção.

O Colaborador não deve utilizar sua conta corporativa de *e-mail* ou sistemas de mensagens instantâneas, para intimidar, assediar, causar constrangimentos, fazer propaganda político-partidária, para incitação à violência, racismo, enviar *e-mail* mal-intencionado, ou para qualquer outro ato ilícito.

Fica terminantemente proibido o uso do serviço de *e-mail* para enviar e/ou receber mensagens contendo pornografia, correntes, spam, arquivos executáveis, conteúdo discriminatório, ataques ou qualquer outro conteúdo indevido.

É proibido enviar ativos de informação sob a gestão da Carpa Family Office para correio eletrônico ou nuvem pessoal.
É proibido utilizar o serviço de *e-mail* ou os sistemas de mensagens instantâneas para trafegar, indevidamente, ativos de informação sensíveis ou sigilosos que pertençam à Carpa Family Office.

Todas as mensagens enviadas por e-*mail* são consideradas comunicação formal da Carpa Family Office.

O envio ou repasse por *e-mail* de material que contenha conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo é também terminantemente proibido, conforme acima aventado, bem como o envio ou repasse de *e-mails* com opiniões, comentários ou mensagens que possam difamar a imagem e/ou afetar a reputação da Carpa Family Office.

Em nenhuma hipótese um Colaborador pode emitir opinião por *e-mail* em nome da Carpa Family Office, ou utilizar material, marca e logotipos da Carpa Family Office para assuntos não corporativos ou após o rompimento do seu vínculo com este, salvo se expressamente autorizado para tanto.

A CARPA FAMILY OFFICE MONITORA O RECEBIMENTO E ENVIO DE MENSAGENS ELETRÔNICAS QUE POSSAM CAUSAR DANOS AOS ATIVOS DE INFORMAÇÃO DA ORGANIZAÇÃO. PORTANTO, MENSAGENS COM ASSUNTOS INDEVIDOS OU QUE CONTENHAM ARQUIVOS ANEXOS COM AS EXTENSÕES HTA, BAT, EXE, COM, SCR, PIF, EXE, AVI, MP3, ENTRE OUTROS, SERÃO MONITORADAS E BLOQUEADAS.

A CARPA FAMILY OFFICE RESERVA O DIREITO DE MONITORAR E IMPEDIR QUANDO NECESSÁRIO O TRÁFEGO EFETUADO ATRAVÉS DAS SUAS REDES DE COMUNICAÇÃO, INCLUINDO ACESSO À INTERNET, USO DO E-MAIL E TELEFONES, DE NOTEBOOKS EM COMODATO OU DOS DESKTOPS DISPONÍVEIS NA CARPA FAMILY OFFICE, BEM COMO COMUNICAR OCORRÊNCIAS EM DESACORDO COM ESTA POLÍTICA AOS DIRETORES EXECUTIVOS E AOS MEMBROS DO COMITÊ EXECUTIVO. O COMPLIANCE TAMBÉM SERÁ AVISADO POR E-MAIL EM CASO DE TENTATIVA DE ACESSO AOS DIRETÓRIOS E LOGINS VIRTUAIS NO SERVIDOR PROTEGIDOS POR SENHA. O COMPLIANCE ELUCIDARÁ AS CIRCUNSTÂNCIAS DA OCORRÊNCIA DESTE FATO E APLICARÁ AS DEVIDAS SANÇÕES.

13. Das Punições

O Colaborador que infringir qualquer uma das normas de segurança expostas nos documentos que compõem esta Política, estará sujeito a punições, desde as mais simples, como advertência verbal ou escrita, até ação judicial. As sanções decorrentes do descumprimento dos princípios ora estabelecidos serão definidas e aplicadas pelo *Compliance*, a exclusivo critério deste, garantido ao Colaborador, contudo, amplo direito de defesa. As sanções acima descritas poderão ser aplicadas sem prejuízo do direito da Carpa Family Office de pleitear indenização pelos eventuais prejuízos suportados, perdas e danos e/ou lucros cessantes, por meio das medidas legais cabíveis.

Cabe ressaltar que algumas normas citadas nos documentos que compõem esta Política são consideradas pela lei como crime. O *Compliance* avaliará os casos de transgressão a presente Política e determinará a aplicação das medidas administrativas e judiciais cabíveis, que poderão levar inclusive à demissão do Colaborador ou abertura de inquérito criminal, sem prejuízo de eventual cobrança de perdas e danos em âmbito civil.

14. Continuidade de Negócios

O Plano de Continuidade de Negócios contempla os principais sistemas e serviços da companhia deverá ser implantado e testado anualmente, contemplando cenários de incidentes, a fim de reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação, de acordo com o documento Plano de Continuidade de Negócios.

15. Arquivamento de Informações

De acordo com o disposto nesta Política, os Colaboradores deverão manter arquivada todos os documentos e informações exigidos pela Resolução CVM n° 21, de 25 de fevereiro de 2021 ("RCVM 21"), conforme alterada, bem como toda a correspondência, interna e externa, todos os papéis de trabalho, relatórios e pareceres relacionados com o exercício de suas funções, em conformidade com o Artigo 34 da RCVM 21, pelo prazo mínimo de 5 (cinco) anos. Adicionalmente, devem ser mantidos pelo mesmo prazo arquivo segregado documentando as operações em que tenha sido contraparte dos fundos de investimento ou das carteiras administradas.

As imagens digitalizadas são admitidas em substituição aos documentos originais, desde que o processo seja realizado de acordo com a lei que dispõe sobre elaboração e o arquivamento de documentos públicos e privados em meios eletromagnéticos, e com o decreto que estabelece a técnica e os requisitos para a digitalização desses documentos, sendo certo que o documento de origem pode ser descartado após sua digitalização, exceto se apresentar danos materiais que prejudiquem sua legibilidade.

16. Treinamento

O Diretor de *Compliance* organizará treinamento anual aos Colaboradores com relação às regras e procedimentos acima, sendo que tal treinamento poderá ser realizado em conjunto com o treinamento anual de Compliance e PLDFT (Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo).

17. Revisão da Política

O Diretor de *Compliance* deverá realizar uma revisão desta Política sempre que necessário, para avaliar a eficácia da sua implantação, identificar novos riscos, ativos e processos e reavaliando os riscos residuais.

A finalidade de tal revisão será assegurar que os dispositivos aqui previstos permaneçam consistentes com as operações comerciais da Carpa Family Office e acontecimentos regulatórios relevantes.

18. Divulgação, Vigência e Validade

Esta Política é apresentada aos Colaboradores, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como promover o seu fiel cumprimento. Essa Política será divulgada por intermédio de mensagem eletrônica (*e-mail*) e será publicada na *intranet*. Qualquer dúvida ou sugestão deve ser encaminhada ao Departamento de Tecnologia e Segurança da Informação.

A presente Política entra em vigor na data de sua publicação e deverá ser revisto e, se necessário, atualizado pelo Compliance no mínimo a cada 24 meses, serão utilizadas como base para sua atualização as legislações, instruções normativas e regulamentações vigentes na data da sua revisão.

19. Considerações Finais

Todas as dúvidas sobre as diretrizes desta Política podem ser esclarecidas com o Compliance da Carpa Family Office.

ANEXO I

CONTRATO DE COMODATO E RESPONSABILIDADE PELA GUARDA E USO DE EQUIPAMENTO

PARTES:

[empresa Carpa] , doravante denominada **CARPA FAMILY OFFICE**

[colaborador], doravante denominado(a) **[ ]**

NOME COMPLETO
CPF

I - DO OBJETO

CLÁUSULA 1ª - Por meio do presente instrumento particular, as partes estabelecem a transferência, pela **CARPA FAMILY OFFICE** ao **[ ],** dos direitos de uso e gozo dos equipamentos e computadores descritos a seguir:

II - DAS RESPONSABILIDADES

CLÁUSULA 2º - O **[ ]** se responsabiliza por manter em perfeito estado de conservação e funcionamento o computador descrito abaixo, cedido pela **CARPA FAMILY OFFICE** em comodato exclusivamente para o desempenho de suas funções.

MARCA: DELL
MODELO: NOTEBOOK DELL INSPIRON
ANO: 2020
DEMAIS INFORMAÇÕES: Intel iX, etc.

CLÁUSULA 3ª - Em caso de dano no equipamento a **CARPA FAMILY OFFICE** poderá efetuar o desconto no valor do equipamento do salário ou distribuição de lucros devido ao **[ ],** conforme o caso, bem como efetuar a cobrança de eventuais valores remanescentes, nos termos do art. 462, §1º da CLT, quando aplicável.

III - DA DESTINAÇÃO E USO

CLÁUSULA 4ª - O **[ ],** está ciente de que o uso do equipamento é estritamente para fins profissionais, estando sujeito à monitoramento e fiscalização da **CARPA FAMILY OFFICE** a qualquer tempo, sem necessidade de aviso prévio.

IV - DA RESCISÃO DO CONTRATO DE TRABALHO OU SAÍDA DE SÓCIO, E DEVOLUÇÃO DO EQUIPAMENTO

CLÁUSULA 5ª - Na hipótese de rescisão do contrato de trabalho, quando da saída do sócio da **CARPA FAMILY OFFICE,** ou em qualquer hipótese quando solicitado pela **CARPA FAMILY OFFICE** , o equipamento deve ser devolvido no prazo de 2 (dois) dias úteis, mediante a assinatura de termos de devolução do equipamento, sob pena do valor do equipamento ser descontado no Termo de Rescisão do Contrato de Trabalho ou de eventuais recursos devidos ao sócio em retirada, sem prejuízo de outras ações judiciais cabíveis.

V - DAS CONDIÇÕES GERAIS

CLÁUSULA 6ª - Este contrato, passa a vigorar a partir da assinatura de ambas as partes.

VI - DO FORO

CLÁUSULA 7ª - As partes elegem o foro da comarca de São Paulo, para dirimir quaisquer controvérsias oriundas do presente contrato.

CLÁUSULA 9ª: As PARTES poderão celebrar o presente instrumento por meio eletrônico, com ou sem certificado digital, a depender da plataforma de custódia escolhida pelas Partes, de modo que assim feito, suas assinaturas por tal meio são vinculantes, eficazes e conferem autenticidade, integridade e validade jurídica a este instrumento, tornando-o título executivo extrajudicial para todos os fins de direitos, nos termos da Lei 14.620, de 13 de julho de 2023.

E por estarem assim justos e acertadas, as Partes firmam o presente Instrumento.

São Paulo, SP, Clique ou toque aqui para inserir uma data.

_____

NOME COMPLETO

_____

CARPA FAMILY OFFICE