POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, CYBER SEGURANÇA E LGPD

Versão Atualizada: 2.0.0 – Fevereiro/2025

POLÍTICA DE CONFIDENCIALIDADE, SEGURANÇA DA INFORMAÇÃO, CYBERSEGURANÇA E LGPD

Objetivo

Contribuir para o aprimoramento da segurança, tanto informacional quanto cibernética da CARPA GESTORA DE RECURSOS LTDA e da CARPA CONSULTORIA FINANCEIRA E GESTAO PATRIMONIAL LTDA (em conjunto "CARPA"), visando garantir a proteção, a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações de sua propriedade e/ou sob sua guarda, e estabelecendo medidas a serem tomadas para identificar e prevenir contingências que possam causar prejuízo para a consecução de suas atividades.

A quem se aplica?

Sócios, diretores e funcionários que participem, de forma direta, das atividades diárias e negócios, representando a gestora e a consultoria da CARPA (doravante, "Colaboradores").

Revisão e Atualização

Esta Política deverá ser revisada e atualizada a cada 2 (dois) anos, ou em prazo inferior, se assim necessário por mudanças legais/regulatórias/autorregulatórias.

Responsabilidades

Os Colaboradores devem atender aos procedimentos estabelecidos nesta Política, informando quaisquer irregularidades ao Diretor de *Compliance* e PLD, que deverá avaliá-las e submetê-las à Alta Administração, conforme o caso.

O Diretor de *Compliance* e PLD deve garantir o atendimento a esta Política, sendo o responsável na CARPA por temas de segurança da informação/cibernética, confidencialidade e LGPD.

Contexto Operacional e de Negócios

Esta política foi elaborada considerando as seguintes premissas e particularidades do modelo operacional e de negócio da CARPA:

- ✓ Todos os sistemas utilizados pela gestora, seja sistemas internos ou de terceiros são acessíveis via *web;*
- ✓ Os fornecedores dos sistemas utilizados pela CARPA se comprometem com disponibilidade, segurança e planos de contingência compatíveis com as necessidades da CARPA;
- ✓ Os colaboradores da CARPA estabelecem tratativas e formalizam seus entendimentos com clientes por meio de ferramentas e aplicativos de mensagens e/ou e-mail corporativo;
- ✓ A gestora aloca recursos mediante a utilização de corretoras/plataformas de investimento acessíveis pela WEB e disponíveis para qualquer dispositivo eletrônico (*laptops*, *smartphones*, *tablets* ou computadores de mesa);
- ✓ O sistema de consolidação de carteiras utilizado pela CARPA identifica os clientes por meio de siglas, dispensando a identificação mediante o preenchimento de cadastro com informações pessoais;
- ✓ Os arquivos contendo informações pessoais e financeiras dos clientes da CARPA são

armazenados em nuvem, com *backups* periódicos não superiores a 7 (sete) dias corridos, podendo ser recompostos solicitando tais informações aos próprios clientes;

- ✓ Os dispositivos eletrônicos (*laptops*, *smartphones*, *tablets*) utilizados no exercício das atividades da CARPA possuem senha de acesso e criptografia;
- ✓ A CARPA utiliza redes sem fio para fornecer acesso à *web* para seus Colaboradores, prestadores de serviço ou visitantes, todas devidamente protegidas por senhas. Em caso de indisponibilidade temporária para acesso à *web*, os Colaboradores utilizam redes/roteadores de redundância;
- ✓ O espaço físico/escritório da CARPA é o local preferencialmente utilizado para as suas atividades, reuniões com clientes, comitês e reuniões comerciais com Colaboradores ou terceiros. Porém, as atividades, rotinas e sistemas da CARPA estão parametrizados para serem passíveis de desempenhados remotamente.

Política de Confidencialidade

São consideradas "Informações Confidenciais" aquelas não disponíveis ao público, que:

- ✓ Identifiquem dados pessoais ou patrimoniais (da CARPA ou de clientes);
- ✓ Sejam objeto de acordo de confidencialidade celebrado com terceiros;
- ✓ Identifiquem ações estratégicas – dos negócios da CARPA, seus clientes ou dos portfólios sob gestão[1];
- ✓ Todas as informações técnicas, jurídicas e financeiras, escritas ou arquivadas eletronicamente, que digam respeito às atividades da CARPA, e que sejam devidamente identificadas como sendo confidenciais, ou que constituam sua propriedade intelectual ou industrial, e não estejam disponíveis, de qualquer outra forma, ao público em geral;
- ✓ Sejam assim consideradas em razão de determinação legal, regulamentar e/ou autorregulatória; e que
- ✓ O Colaborador utiliza para autenticação de sua identidade (senhas de acesso ou crachás), que são de uso pessoal e intransferível.

Não caracteriza descumprimento desta Política a divulgação de Informações Confidenciais: (i) mediante prévia autorização do Diretor de *Compliance* e PLD, (ii) em atendimento a ordens do Poder Judiciário ou autoridade regulatória, administrativa ou legislativa competente, bem como (iii) quando a divulgação se justificar, por força da natureza do contexto da revelação da informação, a advogados, auditores e contrapartes.

Em caso de dúvida, o Colaborador deverá consultar previamente o Diretor de *Compliance* e PLD acerca da possibilidade de compartilhamento da Informação Confidencial.

Política de Segurança da Informação

Os seguintes princípios norteiam a segurança da informação na CARPA:

Confidencialidade: o acesso à informação deve ser obtido somente por pessoas autorizadas, e quando for de fato necessário;

Disponibilidade: as pessoas autorizadas devem ter acesso à informação sempre que necessário;

Integridade: a informação deve ser mantida em seu estado original, visando a protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

[1] Cuja divulgação possa prejudicar a gestão dos negócios, clientes e portfólios a cargo da CARPA, ou reduzir sua vantagem competitiva.

As seguintes diretrizes devem ser seguidas por todos os Colaboradores da CARPA:

- ✓ As informações confidenciais devem ser tratadas de forma ética e sigilosa, e de acordo com as leis e normas internas vigentes, evitando-se mau uso e exposição indevida;
- ✓ A informação deve ser utilizada apenas para os fins sob os quais foi coletada;
- ✓ A concessão de acessos às informações confidenciais deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades;
- ✓ A identificação de qualquer Colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- ✓ Segregação de instalações, equipamentos e informações comuns, quando aplicável;
- ✓ A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento.

Qualquer risco ou ocorrência de falha na confidencialidade e na segurança da informação deve ser reportado ao Diretor de *Compliance* e PLD.

Controles e Obrigações

Identificação, Classificação e Controle da Informação

O Colaborador que recebe ou prepara uma informação pode, se eventualmente necessário, classificá-la como "Confidencial". Para tal conclusão, devem ser considerados as questões de natureza legal e regulatória, de estratégia negocial, os riscos do compartilhamento, as necessidades de restrição de acesso e os impactos no caso de utilização indevida das informações.

Caso haja informação de natureza "Confidencial", o acesso a mesma deve ser restrito e controlado.

Sempre que necessário, contratos de confidencialidade da informação devem ser assinados com terceiros, sob supervisão do Diretor de *Compliance* e PLD, e, se reputado necessário, da assessoria jurídica da CARPA.

A informação deve receber proteção adequada. Em caso de dúvida, o Colaborador deverá consultar o Diretor de *Compliance* e PLD.

O descarte de Informação Confidencial armazenada em meio físico deve ser efetuado utilizando preferencialmente máquina fragmentadora/trituradora de papéis ou incineradora.

Mesa Limpa

Nenhuma Informação Confidencial deve ser deixada à vista nos locais de trabalho dos Colaboradores, mesmo quando trabalhando remotamente. Ademais, ao usar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

Gestão de Acessos

Os serviços de rede, internet e correio eletrônico disponíveis na CARPA são de sua propriedade exclusiva, sendo permitido o uso moderado para fins particulares.

A CARPA poderá, a qualquer momento, mediante prévia aprovação do Diretor de *Compliance* e PLD, e sem obrigação de cientificação prévia:

- ✓ inspecionar conteúdo e registrar o tipo de uso dos *e-mails* feitos pelos usuários;

- ✓ disponibilizar esses recursos a terceiros, caso entenda necessário;
- ✓ solicitar aos usuários justificativas pelo uso efetuado;
- ✓ monitorar acesso a sites, aplicativos etc.;
- ✓ bloquear acesso a sites.

No caso de mudança de área ou desligamento do Colaborador, a respectiva senha de acesso é cancelada, visando ao impedimento de acesso não autorizado pelo ex-Colaborador.

Os equipamentos, ferramentas e sistemas concedidos aos Colaboradores devem ser configurados com os controles necessários para cumprir os requerimentos de segurança aplicáveis à CARPA.

Apenas os Colaboradores devidamente autorizados terão acesso[2] às dependências e sistemas a que estiverem liberados, bem como aos arquivos, diretórios e/ou pastas na rede da CARPA, mediante segregação física e lógica.

Gestão de Riscos, Tratamento de Incidentes de Segurança da Informação, Continuidade de Negócio e *Backups*

Os riscos e incidentes de segurança da informação devem ser reportados ao Diretor de *Compliance* e PLD, que adotará as medidas cabíveis.

O plano de contingência e de continuidade dos principais sistemas e serviços fornecidos por terceiros deve ser objeto de testes, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação. O Diretor de *Compliance* e PLD deve solicitar o resultado de tais testes aos fornecedores de tais sistemas, bem como acompanhar a solução de eventuais deficiências apontadas em tais testes.

No caso de vazamento de informação, ou acesso indevido a informação, o Diretor de *Compliance* e PLD deverá ser imediatamente comunicado, para a tomada das medidas cabíveis[3].

Política de Cybersegurança

As principais ameaças e riscos aos ativos cibernéticos da CARPA são:

- *Malwares* – *softwares* desenvolvidos para corromper os computadores e redes, como:
  - ✓ vírus: *software* que causa danos às máquinas, redes, *softwares* e bancos de dados;
  - ✓ cavalos de troia: aparecem dentro de outro *software*, criando uma entrada para invasão da máquina;
  - ✓ *spywares*: *software* maliciosos que coletam e monitoram as atividades das máquinas invadidas;
  - ✓ *ransomware*: *softwares* maliciosos que bloqueiam o acesso a sistemas e bases de dados, solicitando resgates para restabelecimento do uso/acesso.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito, como, por exemplo:
  - ✓ *pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - ✓ *phishing*: *links* veiculados por e-mails simulando pessoas ou empresas confiáveis que enviam comunicação eletrônica aparentemente oficial para obter informações confidenciais;

[2] Quaisquer exceções deverão ser previamente solicitadas ao Diretor de *Compliance* e PLD.

[3] Podendo variar de simples repreensão pelo acesso, ou mensagem ao destinatário errôneo da mensagem enviada (para que apague em definitivo o seu conteúdo), até o estudo e implementação efetiva de providências judiciais, quando e se for o caso, sem prejuízo da investigação e eventual punição dos Colaboradores envolvidos.

- ✓ *vishing*: simulação de pessoas ou empresas confiáveis para, por meio de ligações telefônicas, obtenção de informações confidenciais;
- ✓ *smishing*: simulação de pessoas ou empresas confiáveis para, por meio de mensagens de texto, obtenção de informações confidenciais;
- ✓ ataques de DDOS (*distributed denial of services*) e *botnets* – ataques visando a negar ou atrasar o acesso aos serviços ou sistemas da instituição;
- ✓ invasões (*advanced persistent threats*) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Controles e Obrigações

Na prestação de seus serviços, a CARPA obtém e lida com informações sensíveis, não disponíveis ao público em geral, e que podem ocasionar perdas irreparáveis em casos de malversação, negligência ou vazamentos[4].

O responsável por tais questões na CARPA é o Diretor de *Compliance* e PLD.

São itens obrigatórios de cybersegurança (empresa):

- o A adequada proteção dos ativos cibernéticos da CARPA, aí incluídos sua rede, sistemas, *softwares*, websites, equipamentos e arquivos eletrônicos.
- o Restrição e controle do acesso e privilégios de usuários não pertencentes ao quadro de colaboradores da CARPA;
- o Invalidar contas de Colaboradores e prestadores de serviço em seu desligamento;
- o Quando necessário, bloquear chaves de acesso de usuários, e, quando necessário, realizar auditoria para verificação de acessos indevidos;
- o Excluir ou desabilitar contas inativas;
- o Fornecer senhas de contas privilegiadas somente a Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;
- o Garantir o cumprimento do procedimento de *backup* para os servidores e ativos cibernéticos, eletrônicos e computacionais da CARPA;
- o Detectar, identificar, registrar e comunicar ao Diretor de *Compliance* e PLD as violações ou tentativas de acesso não autorizadas;
- o Organizar treinamentos relacionados à segurança dos ativos de informação sempre que necessário;
- o Nos casos em que tais serviços e controles acima sejam terceirizados, é necessário que as condições contratuais garantam que o prestador de serviço atesta esta proteção;
- o Caso necessário, a partir de resultados apresentados nos testes de aderência, revisar tais práticas;
- o A CARPA dispõe de segurança nos servidores para acesso à sua rede, visando a manter o ambiente de trabalho disponível e livre de vírus e acessos indesejados. O sistema de prevenção a ataques de vírus é regularmente atualizado;
- o É realizado *backup* de arquivos de forma sistemática. Os dados de *backup* atualizados são

[4] Os riscos potenciais relativos a tais dados envolvem invasões, disseminação errônea ou dolosa, acesso indevido e/ou seu roubo/desvio.

armazenados em local seguro, com monitoramento.

São itens OBRIGATÓRIOS de cybersegurança (Colaboradores):

- Somente enviar mensagens para as pessoas envolvidas no assunto tratado, certificando-se dos endereços de destino escolhidos;
- Somente imprimir as mensagens quando realmente necessário;
- Ao identificar mensagem com título ou anexo suspeito, certificar-se sobre a segurança em abrí-la, para evitar vírus ou códigos maliciosos;
- No caso de recebimento de mensagens que contrariem as regras estabelecidas pela CARPA, NUNCA as repassar, alertando o responsável da sua área e o Diretor de *Compliance* e PLD, se for o caso;
- Ao se ausentar do seu local de trabalho, mesmo quando estiver trabalhando remotamente e mesmo que temporariamente, bloquear a estação de trabalho;
- Quando sair de férias ou se ausentar por períodos prolongados, o Colaborador deve utilizar o recurso de ausência temporária de e-mail;
- Utilizar equipamentos, aplicativos, impressoras, acesso a sites, e e-mail (e demais ferramentas tecnológicas) com a finalidade primordial de atender aos interesses da CARPA[5];
- Tecnologias, marcas, metodologias e quaisquer informações que pertençam à CARPA não devem ser utilizadas para fins particulares, nem repassadas a outrem, ainda que tenham sido obtidas ou desenvolvidas pelo próprio Colaborador em seu ambiente de trabalho;
- Cada Colaborador terá acesso somente a pastas eletrônicas relacionadas à sua área e às pastas comuns a todos os Colaboradores.

São itens VEDADOS de cybersegurança (Colaboradores):

- Enviar e-mail ou acessar sites que promovam a veiculação de mensagens, produtos, imagens ou informações que interfiram na execução das atividades profissionais[6];
- Trocar informações que causem quebra de sigilo bancário e/ou possuam caráter confidencial ou estratégico[7];
- Prejudicar intencionalmente usuários da internet, mediante desenvolvimento de programas, acessos não autorizados a computadores e alteração de arquivos, programas e dados na rede da CARPA;
- Divulgar propaganda ou anunciar produtos ou serviços particulares pelo correio eletrônico da CARPA;
- Alterar qualquer configuração técnica dos *softwares* que comprometam o grau de segurança, ou impeçam/dificultem seu monitoramento pelo Diretor de *Compliance* e PLD;
- Contratar provedores de acesso sem autorização prévia ou ciência do Diretor de *Compliance* e PLD;
- Uso de compartilhadores de informações, tais como redes *Peer-toPeer* (P2P – p. ex., Kazaa, eDonkey, eMule, BitTorrent e semelhantes) nas dependências da CARPA.

Exceções a esta Política de Cybersegurança (Colaboradores):

[5] Os computadores, arquivos, e, arquivos de e-mails corporativos poderão ser inspecionados, **independentemente de prévia notificação ao Colaborador**, a fim de disseminação errônea ou dolosa, acesso indevido e/ou roubo/desvio de informações.

[6] Sendo proibido, sobretudo, conteúdo pornográfico, racista ou ofensivo à moral e aos princípios éticos.

[7] Exceção, é claro, a fluxos de informações necessários para a gestão de fundos e carteiras com instituições envolvidas nas operações dos clientes.

- Caso haja uso de equipamentos ou dispositivos eletrônicos de propriedade dos colaboradores para desempenhar suas atividades na CARPA, estes se comprometem a adotar as medidas de segurança anteriormente citadas a fim de preservar seus equipamentos e minimizar o risco de comprometimento de segurança às informações sensíveis da CARPA, seus clientes e parceiros de negócio, podendo utilizar tais equipamentos para os diversos fins que considerar pertinentes;
- É facultado ao Diretor de *Compliance* e PLD autorizar exceções à esta política, devendo estar formalizadas por e-mail.

Política de Proteção de Dados Pessoais (LGPD)

A CARPA, no exercício de suas atividades, tem e/ou pode vir a ter acesso a dados pessoais, conforme definidos na Lei n.º 13.709, de 14 de agosto de 2018 ("LGPD").

O tratamento de tais dados é feito nos estritos limites e finalidades da lei e da regulação aplicável (especialmente, sem limitação, as normas da CVM relativas a cadastro e identificação de clientes e operações), dado que o acesso de que aqui se trata é condição obrigatória para o desempenho das atividades da CARPA junto ao público investidor: assim, seu acesso e tratamento se dá em conformidade com estrutura, escala e ao volume de operações da CARPA, bem como à sensibilidade dos dados tratados.

Os dados pessoais, desta forma, são coletados e armazenados apenas e tão-somente para estrito cumprimento da legislação e regulação aplicável às atividades da CARPA, sendo absolutamente vedada a sua destinação diversa pela CARPA e/ou quaisquer de seus Colaboradores: o seu eventual uso compartilhado com reguladores e autoridades poderá ser realizado somente nos estritos termos e limites das normas vigentes aplicáveis à CARPA, e para estrito cumprimento destas.

O tratamento e armazenamento dos dados pessoais recebidos durará pelo tempo em que perdurar o relacionamento entre a CARPA e o(s) titular(es) dos dados pessoais, sempre respeitando simultaneamente o prazo determinado pelas normas vigentes a elas aplicáveis.

As informações de contato e responsáveis da CARPA a esse respeito encontram-se em seu *website*, cabendo ao Diretor de *Compliance* e PLD supervisionar Colaboradores e zelar pelo tratamento de tais dados, sempre resguardados os direitos do titular contemplados no art. 18 da LGPD, quais sejam:

- ✓ confirmação, para o titular dos dados pessoais, da existência do tratamento destes;
- ✓ acesso aos seus dados em poder da CARPA;
- ✓ correção de dados incompletos, inexatos ou desatualizados;
- ✓ anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD;
- ✓ portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- ✓ eliminação dos dados pessoais tratados com o consentimento do titular (exceto, nos termos do art. 16 da LGPD, nas hipóteses de (a) cumprimento de obrigação legal ou regulatória pela CARPA, (b) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos na LGPD, ou (c) uso exclusivo da CARPA, vedado seu acesso por terceiro, e desde que anonimizados os dados);
- ✓ informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

- ✓ informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- ✓ revogação do consentimento.

Nas hipóteses em que o consentimento para o tratamento de dados pessoais for necessário, se houver mudanças da finalidade para o tratamento de dados pessoais não compatíveis com o consentimento original, a CARPA deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

- ✓ verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
- ✓ fim do período de tratamento;
- ✓ comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento; ou
- ✓ determinação da autoridade nacional, quando houver violação ao disposto na LGPD.

Testes de Aderência dos Controles

A efetividade destas Políticas é verificada por meio de testes periódicos dos controles existentes, com intervalos não superiores a 1 (um) ano, sob responsabilidade do Diretor de *Compliance* e PLD e reportados à Alta Administração.

Os testes[8] devem verificar se:

- ✓ Os recursos humanos e computacionais são adequados ao porte e às áreas de atuação;
- ✓ Há adequado nível de confidencialidade e acessos às informações confidenciais, com identificação de pessoas que tem acesso a estas informações;
- ✓ Há segregação física e lógica;
- ✓ Os recursos computacionais, de controle de acesso físico e lógico, estão protegidos;
- ✓ A manutenção de registros permite a realização de auditorias e inspeções, bem como o cumprimento das obrigações relativas à LGPD.

[8] Que podem ser realizados por terceiros, ou objeto de obrigação contratual, passível de reporte por prestadores de serviço, provedores de dados, aplicativos e ferramentas/*softwares*. Tais conteúdos podem ser passíveis de compor o relatório anual de *Compliance* exigido pela regulação aplicável da CVM.