Política de Proteção de Dados e Privacidade

Janeiro 2025

Ficha de Controle da Política

Titulo	Política de Proteção de Dados e Privacidade
Status	Versão inicial
Área Proprietária do Procedimento	Tecnologia da Informação
Escopo de Geográfia	Brasil

Histórico de Versões

Versão	Aprovado por	Data da aprovação	Resumo das alterações
1.0	Diretoria	30/01/2025	Versão inicial

Sumário

1. Escopo

Esta Política de Proteção de Dados e Privacidade ("Política") aplica-se:

- À BCP Distribuidora de Valores mobiliários Ltda, adiante denominada "BCP".

- A todos os colaboradores da BCP, bem como consultores e terceiros contratados, independentemente de sua localização, função, cargo ou grau, especialmente aqueles que possuem acesso a Dados Pessoais, os quais são coletivamente mencionados neste documento como "Áreas de Negócios" e/ou "Colaboradores".

Esta Política tem como objetivo estabelecer normas de boas práticas que a BCP utiliza no processamento de Dados Pessoais, bem como seu compromisso com a segurança, a privacidade e a transparência no tratamento desses dados.

A presente Política descreve os Dados Pessoais coletados pela BCP, como eles são usados, armazenados e compartilhados, bem como os direitos dos titulares em relação a esses dados. O cumprimento desta Política é obrigatório e deve ser lida e interpretada em conjunto com outros documentos pertinentes da BCP, especialmente o Código de Ética e Conduta e o Manual de Segurança da Informação.

2. Definições

Titular de Dados: Qualquer indivíduo a quem se refere os Dados Pessoais que são objeto de tratamento, tais como funcionários, partes relacionadas, clientes, fornecedores e outros com quem a BCP conduza algum negócio ("Titular(es)").

Dados Pessoais: Toda e qualquer informação relacionada a uma pessoa natural, identificada ou identificável, como nome, sobrenome, data de nascimento, idade, contato pessoal, (como por exemplo, mas sem se limitar: endereço residencial ou eletrônico, número de telefone), podendo incluir dados de localização, certificações de habilidades e ou atributos, informações relacionadas a cargo, salário e ou funções, número de IP, dados acadêmicos, histórico de compras, operações realizadas entre outros.

Dados Sensíveis: Informações que estejam relacionadas às características da personalidade do indivíduo e de suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

Tratamento de Dados: Qualquer ação possível feita com Dados Pessoais em nome da BCP, tais como coleta, registro, divulgação, manipulação, atualização, organização, arquivamento, destruição e/ou, simplesmente, manutenção ou armazenamento de Dados Pessoais - seja em papel ou em formato eletrônico.

Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, pelos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Dados Anonimizados: dados relativos a umtitular que não possa ser identificado, considerando a utilização de meios razoáveis e disponíveis na ocasião de seu tratamento.

DPO: *Data Protection Officer*, pessoa indicada pela BCP que atua como canal de comunicação entre ostitulares e demais interessados.

3. Princípios

Os princípios e diretrizes que norteiam a atuação da BCP no tratamento de dados, em conformidade com a legislação local em vigor, são os seguintes:

3.1 Garantia dos direitos fundamentais

A BCP tem como princípio primordial o tratamento de dados em estrita conformidade legal, garantida a proteção de direitos fundamentais como a privacidade, intimidade, honra, direito de imagem e a dignidade.

3.2 Finalidade e compatibilidade

A coleta e tratamento de dados pela BCP baseia-se em propósitos legítimos, específicos, explícitos e informados aotitular, e é compatível com as finalidades pretendidas.

3.3 Limitação ao mínimo necessário

A coleta de dados pela BCP é limitada ao mínimo necessário para os fins pretendidos. A BCP não deve coletar informações além daquelas que precisa. Onde possível, as informações coletadas devem ser anonimizadas.

3.4 Governança dos dados

As informações coletadas devem ser protegidas de acessos não autorizados ou ilegais, devendo a BCP estabelecer medidas técnicas e organizacionais para garantir tal segurança, assim como os direitos dostitulares, especialmente (i) a de consultas facilitada e gratuita sobre a forma do tratamento dos dados; (ii) exatidão, clareza, relevância e atualização dos dados; (iii) acesso, sempre que necessário, à prestação de contas, a fim de comprovar a adoção de medidas de proteção dos dados.

4. Diretrizes

Ao conduzir qualquer tratativa, a BCP tem acesso a determinados dados de indivíduos. Por isso, a BCP estabelece as seguintes diretrizes para garantir a efetiva aplicação dos princípios previstos nesta Política.

4.1 Coleta de dados

A BCP coleta dados sempre que qualquer indivíduo (i) contrata ou usa qualquer um dos seus produtos ou serviços; (ii) navega no seu website e (iii) entra em contato através dos canais de comunicação disponíveis pela BCP.

Também há coleta de dados quando (i) a BCP realiza negócios com parceiros, fornecedores e prestadores de serviços; (ii) quando um candidato se inscreve em um processo seletivo promovido pela BCP; e (iii) um novo colaborador é admitido.

Os dados coletados são aqueles necessários para a realização de suas finalidades, em cumprimento da legislação em vigor.

Toda coleta de dados deve ser justificável. Geralmente, a coleta é justificada com base em uma ou mais das seguintes hipóteses:

a) Necessário para que a BCP execute um contrato ou os procedimentos preliminares a ele relacionados.
b) Necessário para que a BCP cumpra com suas obrigações legais ou regulatórias.
c) Interesse legítimo do titular no exercício regular do seu direito, ou prestação de serviços que venham a beneficiá-lo.
d) Consentimento expresso do titular, de forma livre, informada e inequívoca.

Todos os Colaboradores da BCP que realizam a coleta de dados devem observar as condições aqui previstas, sendo que, quando não tiverem certeza se alguma das condições se aplica, deverão procurar o Departamento de Compliance ou o DPO.

4.1.1 Dados Sensíveis

O tratamento de dados sensíveis deve ocorrer apenas em circunstâncias onde a BCP for capaz de justificar a coleta e o tratamento dessas informações, fundamentada em ao menos um dos seguintes motivos:

a) Houver o consentimento explícito e informado;
b) O indivíduo de outra forma tornou a informação pública;
c) A informação é necessária para:
    i) cumprir direitos ou obrigações legais ou regulatórias da BCP.
    ii) proteger os interesses vitais do indivíduo.
    iii) o exercício regular de direitos.
    iv) prevenir fraudes e garantir a segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

Deve-se ter especial atenção com relação às informações consideradas sensíveis. A BCP estabelece níveis apropriados de segurança e acesso do usuário em relação a essas informações.

4.2 Processamento e tratamento

No tratamento de dados, a BCP deve garantir que as informações de indivíduos sob o seu controle não sejam removidas ou copiadas sem o seu conhecimento ou permissão, tampouco sejam acessadas por terceiros que não tenham autorização para acessar tais informações. As medidas de segurança adotadas para evitar o acesso de Pessoa não Autorizada incluem:

a) Proteger ou bloquear dispositivos remotos, laptops, cartões de dados etc. que contenham quaisquer Dados Pessoais ou outras informações confidenciais fora do horário comercial.

b) Tomar medidas para que os documentos contendo Dados Pessoais não sejam deixados em suas mesas, impressoras, scanners ou fotocopiadoras.

Dispositivos pessoais não devem ser usados para processar Dados Pessoais de indivíduos que possuam relacionamento com a BCP, exceto se através de aplicativos previamente aprovados pela BCP.

Todos os arquivos e informações da BCP devem ser armazenados e mantidos nos sistemas homologados e utilizados pela própria BCP, de modo que esta possa assegurar a segurança através de backup e de outras medidas que permitam a recuperação, quando necessário.

4.3 Compartilhamento e transferência de dados

Para desenvolver sua atividade econômica, a BCP é obrigada a compartilhar certos Dados Pessoais com terceiros, tais como fornecedores, provedores de TI, empresas de infraestrutura de mercado financeiro (por exemplo: B3), consultores profissionais e outros parceiros de negócios.

Todo compartilhamento e/ou transferência de Dados Pessoais deve ser feito observando-se se (i) a BCP possui justificativa para fazê-lo; e (ii) se o receptor possui medidas técnicas e organizacionais apropriadas para garantir a segurança, a privacidade e a transparência no tratamento desses dados.

É vedado o compartilhamento de informação, dado ou software com Pessoas não Autorizadas, de dentro e ou de fora da BCP. Dúvidas sobre o compartilhamento devem ser previamente direcionadas ao Departamento de Compliance ou ao DPO da BCP.

Deverá ser observada a existência de contrato por escrito com o terceiro destinatário antes que ele tenha acesso às informações, especificando, entre outras coisas, qual a finalidade do compartilhamento e em que momento os dados não serão mais necessários. Na medida do possível, as informações devem ser criptografadas durante o trânsito, de forma a mitigar o risco de vazamento.

4.3.1 Transferência de informações para fora do Brasil

Se o destinatário dos Dados Pessoais estiver localizado fora do Brasil, pode ser necessário cumprir requisitos adicionais para garantir a segurança das informações.

4.4 Retenção e armazenamento

A BCP usará os dados coletados por quanto tempo for necessário para satisfazer as finalidades correlatas, assim como para cumprir as várias obrigações legais, regulatórias ou decorrentes de acordos e contratos firmados com funcionários, partes relacionadas, clientes, fornecedores e outros.

A retenção de informações é importante para garantir que a BCP possa (i) responder a eventos imprevistos, como litígios ou incidentes decorrentes de riscos inerentes à atividade, inclusive quando ocorrer caso fortuito ou de força maior; e (ii) proteger o interesse dos titulares de dados.

Dados Pessoais devem ser mantidos atualizados e precisos, de forma a atender aos requisitos regulatórios vigentes. Ocorrendo qualquer incidente de utilização de dados desatualizados, tão logo seja de conhecimento da BCP, estas informações deverão ser atualizadas.

Para cada tipo de informação haverá um período de retenção obrigatório. Havendo necessidade de orientação sobre o prazo de retenção de determinada informação, os Colaboradores da BCP deverão entrar em contato com o Departamento Jurídico ou com o DPO.

Ao término de toda e qualquer relação de emprego, prestação de serviços ou qualquer compromisso assumido entre a BCP e um colaborador, este deverá devolver todas e quaisquer informações que tenha retido consigo relacionadas aos negócios da BCP.

4.5 Exclusão

Ressalvadas as hipóteses previstas nesta Política, todos os Dados Pessoais devem ser descartados de forma adequada ao final do período de retenção, ou quando não forem mais necessários.

Para garantir a segurança das informações, é importante seguir as etapas abaixo:

- Em se tratando de descarte de informações contidas em cópias eletrônicas (por exemplo, em discos rígidos, mídias de armazenamento entre outros) ou em equipamentos de tecnologia, é obrigatório o envolvimento da área de TI, que ficará encarregada de destruir as informações e/ou equipamento.

- Para as informações contidas em material impresso, os Colaboradores da BCP devem revisar regularmente o acervo e, sempre que possível, realizar o descarte, que deve ser feito através de máquinas trituradoras e fragmentadoras de papel disponíveis na BCP. O gerente/diretor da área deve sempre ser informado sobre a exclusão de qualquer dado pessoal contido em material impresso e será o responsável por identificar eventuais necessidades especiais quanto ao tratamento desses dados. É vedada a retenção de informações em lugares expostos.

5. Direito dos titulares

A BCP deve assegurar a todos os titulares os seguintes direitos:

- Confirmar a existência de tratamento de seus Dados Pessoais.
- Acessar seus Dados Pessoais.
- Corrigir Dados Pessoais incompletos, inexatos ou desatualizados.
- Ter seus dados anonimizados, bloqueados ou eliminados, se forem desnecessários, excessivos ou tratados em desconformidade com a legislação em vigor.
- Portabilizar os Dados Pessoais a outro fornecedor de produto ou serviço.
- Obter informações sobre as entidades públicas e privadas com as quais a BCP compartilhou seus Dados Pessoais.
- Obter informações sobre as consequências caso não autorize o tratamento de seus Dados Pessoais pela BCP.
- Revogar o seu consentimento, a qualquer tempo, para o tratamento de seus Dados Pessoais.

A solicitação de quaisquer dos direitos previstos na legislação em vigor e nesta Política pode ser direcionada ao departamento de compliance através do e-mail: compliance@bcpsecurities.com

6.Segurança e Governança Corporativa

As informações coletadas pela BCP trafegam e são armazenadas de forma segura, com uso de criptografia. Os dados são de uso exclusivo da BCP e de seus parceiros.

A BCP atua de forma consciente tendo como pilares, além de outros previstos nesta Política (i) a confidencialidade das informações; (ii) a disponibilidade; e (iii) o desempenho.

A alta administração da BCP tem ciência da importância da presente política, na qual se compromete com a melhoria contínua dos procedimentos ora relacionados juntamente com o DPO.

Dentre as principais áreas e responsabilidades, destacam-se:

6.1 DPO

Esclarecer dúvidas relativas a esta Política e à sua aplicação. Receber reclamações e quaisquer comunicações de indivíduos relacionadas ao processamento de dados. Receber comunicações da Autoridade Nacional de Proteção de Dados (“ANPD”) e adotar providências. Orientar os Colaboradores da BCP a respeito das práticas a serem tomadas em relação a privacidade e proteção de Dados Pessoais.

6.2 Departamento de Compliance

Estabelecer procedimentos e controles internos para assegurar o cumprimento dos princípios e diretrizes previstos nesta Política. Acompanhar os normativos expedidos pelos órgãos reguladores sobre privacidade e proteção de dados e verificar a aplicabilidade na estrutura interna da BCP.

6.3 Departamento Jurídico

Esclarecer dúvidas relativas à legislação e regulamentação pertinente. Gerenciar eventuais requisições de informações junto ao DPO. Gerenciar processos judiciais, administrativos ou regulatórios que envolvam a BCP e/ou partes interessadas, que impliquem e ou tenham relação com os termos desta Política. Elaborar ou revisar os contratos com terceiros, assegurando que os princípios estabelecidos nesta Política sejam previstos e respeitados.

6.4 Departamento de TI

Manter sistemas, processos e infraestrutura de TI que (i) assegurem integridade, segurança e disponibilidade dos dados e dos sistemas de informação utilizados pela BCP; (ii) sejam robustos e adequados às necessidades e às eventuais mudanças do modelo de negócio, tanto em circunstâncias normais quanto em períodos de estresse; e (iii) incluam mecanismos de proteção e segurança da informação, com vistas a prevenir, detectar e reduzir a vulnerabilidade aos ataques digitais.

6.5 Demais Áreas De Negócios e Colaboradores

Observar e zelar pelo cumprimento da presente Política e, quando necessário, acionar DPO da BCP para esclarecer situações que envolvam conflito com os termos aqui previstos.

7. Gerenciamento de Riscos

O vazamento de dados é o principal risco aos preceitos previstos nesta Política. É considerado vazamento qualquer evento que possibilite outras pessoas, além daquelas autorizadas, a ter acesso a Dados Pessoais armazenados pela BCP, seja em meio físico ou eletrônico.

O vazamento de dados pode envolver, por exemplo, mas sem se limitar:

- A perda de um laptop, pasta, pen drive ou dispositivo móvel que contenha Dados Pessoais;
- Envio por e-mail de uma lista de clientes ou funcionários para o destinatário incorreto;
- fornecimento de um login de sistema a um usuário não autorizado;
- Um ataque de *phishing*; ou
- Um evento de *hacking* ou alguma outra forma de ataque cibernético.

Na ocorrência de qualquer uma das hipóteses acima ou de outra não prevista que importe potencial risco de vazamento de dados, o DPO deve ser imediatamente informado, com o máximo de detalhes possíveis.

Violações significativas à presente Política devem ser respondidas de forma eficaz e oportuna pela Diretoria da BCP, com a implementação e o monitoramento de processos, que incluem as seguintes etapas:

- A documentação do incidente, indicando a causa, quando possível.
- A atribuição de classificação de impacto apropriada.
- O escalonamento e o plano de ação.

Tais violações serão consideradas eventos de risco, cabendo ao DPO informar a diretoria da BCP para devido registro, classificação, escalonamento e gestão do plano de ação.

O registro será realizado, sendo obrigatório informar: (i) data da ocorrência; (ii) data da identificação do vazamento; (iii) impacto; (iv) resumo do evento; (v) quantificação financeira da perda ou de potencial perda.

Os eventos são classificados com relação ao impacto de acordo com os critérios adotados pela BCP. Para o seu grau de relevância serão considerados aspectos como comprometimento de dados de clientes e impacto ao sistema financeiro.

Todos os Colaboradores da BCP são orientados e possuem canal aberto para, havendo qualquer suspeita de descumprimento dos princípios e diretrizes desta Política, bem como eventuais vulnerabilidades, comunicar ao superior imediato, à área de Compliance e ao DPO. Nenhum Colaborador deverá investigar por conta própria, ou tomar ações para se defender de eventual descumprimento desta Política, a não ser que seja instruído desta forma pelo DPO. O DPO, juntamente como diretoria estão capacitados para conter as exposições, analisar os impactos da BCP e conduzir investigações, coletando evidências para ações corretivas.

8. Classificação de Dados

Para fins desta Política, a classificação de dados se refere à restrição quanto ao acesso e à disponibilidade de uma informação ou dados sensíveis, cujas classificações podem ser observadas a seguir:

Classificação	Descrição	Exemplos
Secreto	Informações críticas para a BCP e seus negócios, em que o acesso é permitido apenas a pessoal autorizado. Informações para as quais a divulgação potencial ou comprometimento da integridade das informações secretas (interna ou externamente) causaria sérios danos financeiros ou de reputação, perda significativa de vantagem competitiva, sanção regulatória ou ação legal.	Estratégias de negociação do cliente; Dados da Folha de Pagamento; Detalhes da conta bancária; Dados da folha de pagamento; Informações de Identificação Pessoal; Endereço residencial; Dados legalmente privilegiados; Propriedade Intelectual (IP) Proprietária da BCP.

Classificação	Descrição	Exemplos
	Observação: algumas informações só podem ser consideradas secretas por um curto período.	Penetração de Perímetro de TI / Avaliações de Vulnerabilidade; Código-fonte, designs ou modelos algorítmicos; Fusões ou aquisições
Confidencial	Informações de propriedade da BCP e seus negócios e relacionadas a atividades/dados confidenciais/restritos, em que o acesso de todos os funcionários não é necessário ou apropriado. O acesso a informações confidenciais só é exigido por aqueles com uma base de conhecimento permitida para cumprir seus deveres. A possível divulgação ou comprometimento da integridade de Informações confidenciais (interna ou externamente) seriam consideradas passíveis de causar danos financeiros ou de reputação moderados, perda de vantagem competitiva e/ou maior escrutínio regulatório. Observação: as informações transacionais pessoais e não públicas devem ser classificadas como, no mínimo, Confidenciais.	Dados de negociação do cliente, por exemplo ordens, execuções, pós-negociação, Informações de negociação do Cliente, Contratos do cliente, Detalhes de contato do cliente, Resultados e relatórios de auditoria, Contratos Jurídicos / Fornecedores, Informações do cliente, Remuneração do Pessoal.

Uso interno	As informações de Uso Interno estão relacionadas às operações da BCP, comunicações internas não confidenciais e comunicações gerais apropriadas para distribuição em toda a organização. A divulgação ou comprometimento da integridade das informações de Uso Interno seria considerado improvável de resultar em um impacto material para a BCP, seus clientes ou seus parceiros de negócios se expostos a pessoas não autorizadas, mas poderia fornecer conhecimento das operações internas da BCP que podem não ser apropriado para não funcionários. As informações de Uso Interno podem ser enviadas para fora da organização quando apropriado (por exemplo, para terceiros onde o trabalho foi terceirizado) se a autorização do proprietário das informações/dados tiver sido adquirida.	Acessar documentos não classificados como Confidenciais ou Secretos, Anúncios internos BCP nomes e detalhes telefone da equipe, Funções / Cargos, Organogramas, Comunicações e anúncios internos (seja para um ou muitos destinatários) não classificados como Confidencial ou Secreto Agendas/Atas de reuniões não classificadas como Confidenciais ou Secretas
Público	Informações que já estão ou foram autorizadas para o domínio público, ou informações para as quais a divulgação pública não teria impacto negativo ou consequências para a BCP, seus clientes ou parceiros de negócios.	Materiais de marketing, Anúncios de emprego externos, Anúncios públicos, Informações sobre os sites da BCP acessíveis ao público, Publicações irrestritas.

9. Cultura de Privacidade

A presente Política se aplica a todas as Áreas de Negócios e Colaboradores da BCP e deve ser disponibilizada em canal aberto e de fácil acesso.

A BCP, sempre que possível e quando relevante, viabilizará ações de conscientização e publicidade acerca do tema.

10. Gerenciamento da Política

10.1 Revisão

A presente Política deve ser revisada e atualizada sempre que necessário. Qualquer alteração que seja considerada substancial deve ser aprovada pela Diretoria da BCP.

10.2 Violação da Política

A violação desta Política pode resultar na concretização de riscos, o que pode levar a danos significativos para a BCP, incluindo, mas não se limitando, a perdas financeiras, multas regulatórias, danos à reputação e perda de negócios.

Em caso de violação desta Política, o colaborador infrator poderá sofrer penalidades, que serão estabelecidas pela Diretoria, em função da gravidade da ocorrência e em função da reincidência ou não no descumprimento.