BALUARTE CAPITAL GESTÃO DE RECURSOS LTDA.

POLÍTICA DE PRIVACIDADE

Data-Base: 31 de dezembro de 2022

POLÍTICA DE PRIVACIDADE

Esta Política de Privacidade refere-se à utilização dos serviços a serem prestados por BALUARTE CAPITAL GESTÃO DE RECURSOS LTDA., devidamente inscrita no CNPJ/MF sob nº 25.297.476/0001-67 ("Baluarte"), e tem como objetivo fornecer uma visão transparente das práticas relacionadas à coleta, ao uso, ao armazenamento e ao tratamento dos Dados Pessoais divulgados pelo Titular.

A Baluarte coleta (ou pode coletar) e utiliza alguns Dados Pessoais que pertencem àqueles que celebram contratos, de qualquer natureza, com a Baluarte, que utilizam o site e os sistemas operados, contratados ou de propriedade da Baluarte ("Banco de Dados Baluarte"). Ao fazê-lo, a Baluarte, na qualidade de Controladora desses dados, sujeita-se às disposições da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

A Baluarte cuida da proteção dos Dados Pessoais e, por isso, disponibiliza esta Política de Privacidade, que contém informações importantes sobre: (i) quais são e como são utilizados os dados coletados, (ii) compartilhamento de dados com terceiros, (iii) armazenagem e tratamento de dados, (iv) direitos do Titular em relação aos seus Dados Pessoais; (v) medidas de segurança no tratamento de dados, e (vi) dados de contato com a Baluarte.

1. Quais dados são coletados

1.1. O Sistema Baluarte coleta (ou pode coletar) os seguintes tipos de dados dos Titulares:

Dados Pessoais	Quaisquer dados que permitam a identificação pessoal do Titular. Os Dados Pessoais incluem, entre outros, o nome completo, nacionalidade, filiação, estado civil, profissão, endereço, e-mail, número de telefone, RG/RNE e CPF, dados bancários e financeiros.

Dados de Acesso	Informações coletadas de Titulares: inclui, dentre outros, o navegador de acesso do Titular; endereço do protocolo de Internet (IP); data e hora do acesso; e as eventuais ações do Titular nos sistemas da Baluarte. Comunicação entre Titular e a Baluarte: inclui quaisquer comunicações havidas entre a Baluarte e o Titular por e-mail e/ou telefone, bem como qualquer rede social, incluindo, mas não se limitando a WhatsApp e correspondência física e virtual.
Titular	Toda pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

1.2. A Baluarte não coleta e não utiliza Dados Pessoais considerados sensíveis conforme a LGPD. Eventualmente, se forem necessários, Dados Pessoais considerados sensíveis somente serão disponibilizados pelo Titular mediante seu consentimento específico e destacado.

1.3. Em qualquer caso, o tratamento de Dados Pessoais sensíveis somente ocorrerá para atender a finalidades específicas expressas em lei.

2. <u>Como são utilizados os dados coletados</u>

2.1. A Baluarte utiliza os dados coletados para as seguintes finalidades:

Utilização de Dados Pessoais e Dados e Acesso	Quaisquer Dados Pessoais e Dados de Acesso poderão ser utilizados pela Baluarte exclusivamente para o desenvolvimento de suas atividades profissionais, nos termos de sua contratação.
Processamento de Dados	A Baluarte poderá processar os Dados Pessoais e os Dados de Acesso de forma automatizada e codificada, a fim de organizar e estruturar esses dados, para gerar informações e estatísticas gerais não individualizadas para uso próprio e melhor desenvolvimento de suas atividades ("**Dados Gerais**").

Ligações telefônicas e envio de e-mail e notificações	A Baluarte poderá ligar para os Titulares e/ou enviar-lhes e-mails ou notificações com alertas e comunicados relacionados aos serviços contratados.

3. Compartilhamento de dados com terceiros

3.1. Os dados coletados do Titular poderão ser compartilhados com terceiros, nas seguintes hipóteses:

Ordem judicial ou requisição de autoridade competente	A Baluarte poderá compartilhar os dados coletados do Titular quando solicitados (i) por meio de ordem judicial, ou (ii) por requisição de autoridade governamental competente nos termos da legislação.
Novas Funcionalidades	Quando e se houver a necessidade de compartilhamento dos Dados Pessoais do Titular com terceiros, com a finalidade de oferecer uma nova funcionalidade ou serviço ao Titular, ele será notificado para que autorize ou não o compartilhamento. Caso o Titular opte por não autorizar o compartilhamento, seus Dados Pessoais não serão transmitidos ao terceiro.
Novas parcerias	Com o objetivo de estabelecer novas parcerias, a Baluarte poderá compartilhar os Dados Gerais com potenciais parceiros, que não terão acesso aos Dados Pessoais dos Titulares.
Análise de Mercado	Os Dados Gerais poderão ser utilizados pela Baluarte para construção de uma análise de mercado, que poderá ser compartilhada com terceiros, sem a identificação dos Titulares.

3.2. Em nenhum caso, os Dados Pessoais dos Titulares serão objeto de cessão a terceiros pela Baluarte.

3.3. Em qualquer caso, o compartilhamento de Dados Pessoais observará todas as leis e regras aplicáveis, buscando sempre garantir a segurança dos dados de Titulares, observados os padrões técnicos empregados no mercado.

4. Armazenagem e tratamento de dados

4.1. Os Dados Pessoais coletados pela Baluarte são armazenados e utilizados por período que corresponda ao necessário para atingir as finalidades elencadas neste documento e que considere os direitos de seus Titulares, os direitos do Controlador do Banco de Dados Baluarte e as disposições legais ou regulatórias aplicáveis.

4.2. Uma vez expirados os períodos de armazenamento dos Dados Pessoais, eles serão removidos da base de dados ou anonimizados, salvo nos casos em que houver a possibilidade ou a necessidade de armazenamento em virtude de disposição legal ou regulatória.

5. Direitos do Titular

5.1. O Titular possui os seguintes direitos, conferidos pela LGPD:

Direitos do Titular	Confirmação da existência de tratamento; acesso aos dados; correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na lei; 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 casos previstos em lei; 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. É importante destacar que, nos termos da LGPD, não existe um direito de eliminação de dados tratados com fundamento em bases legais distintas do consentimento, a menos que os dados sejam desnecessários, excessivos ou tratados em desconformidade com o previsto na lei.
Como o titular pode exercer seus direitos	Para garantir que o Titular que pretende exercer seus direitos é, de fato, o titular dos dados pessoais objeto da requisição, a Baluarte poderá solicitar documentos ou outras informações que possam auxiliar em sua correta identificação, a fim de resguardar direitos próprios e de terceiros. Isto somente será feito, porém, se for absolutamente necessário, e o requerente receberá todas as informações relacionadas.

6. Medidas de segurança no tratamento de dados pessoais

6.1. A Baluarte emprega medidas técnicas e organizativas aptas a proteger os Dados Pessoais de acessos não autorizados e de situações de destruição, perda, extravio ou alteração desses dados.

6.2. Entre as medidas de segurança adotadas, destacam-se as seguintes: (i) Os dados de Titulares são armazenados em ambiente seguro; (ii) limita-se o acesso aos dados de Titulares, de modo que terceiros não autorizados não possam acessá-los; (iii) a Baluarte mantém registros de todos aqueles que têm, de alguma forma, contato com os dados.

6.3. Ainda que adote tudo o que está ao seu alcance para evitar incidentes de segurança, é possível que ocorra algum problema motivado exclusivamente por um terceiro - como em caso de ataques de *hackers* ou *crackers* ou, ainda, em caso de culpa exclusiva do

Titular, que ocorre, por exemplo, quando ele mesmo transfere seus dados a terceiro. Assim, embora a Baluarte, em geral, seja responsável pelos Dados Pessoais que trata, ela se exime de responsabilidade caso ocorra uma situação excepcional como essas, sobre as quais não tenha nenhum tipo de controle.

6.4. A Baluarte utiliza internet dedicada, mecanismo de conexão criado especialmente para o mundo corporativo, o que garante uma melhor qualidade na prestação de seus serviços, bem como menor tempo de reparo em caso de interrupções.

6.5. A fim de garantir proteção aos seus sistemas e aos dados que armazena, a Baluarte adota o uso de diversas ferramentas de cibersegurança, dentre elas:

(i) Sistema de firewall na rede da Gestora;
(ii) Aprovação de acesso em 2 (duas) ou mais etapas, para operações bancárias;
(iii) Uso de antivírus em seus equipamentos; e
(iv) Sistema de segurança para armazenamento e compartilhamento de senhas.

6.6. A Baluarte não possui servidor interno, efetuando o armazenamento de todos os dados em nuvem, por meio de diversas plataformas, como Dropbox, G Suite, e *Softwares as a Service* – SaaS, como Comdinheiro, Advent Geneva e Quickbooks.

6.7. A Gestora possui controle físico acerca do acesso de seus Colaboradores e/ou Prestadores de Serviços às suas dependências, por meio de registro de entrada e saída de qualquer pessoa que tenha acesso ao ambiente de serviços da Baluarte.

6.8. De qualquer forma, caso ocorra qualquer tipo de incidente de segurança que possa gerar risco ou dano relevante para qualquer dos Titulares, a Baluarte comunicará os afetados e a Autoridade Nacional de Proteção de Dados acerca do ocorrido, em conformidade com o disposto na LGPD.

7. Reclamação a Autoridade Nacional de Proteção de Dados

7.1. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, os Titulares de Dados Pessoais que se sentirem, de qualquer forma, lesados, podem apresentar reclamação à Autoridade Nacional de Proteção de Dados.

8. Como entrar em contato com a Baluarte

8.1 Para esclarecer quaisquer dúvidas sobre esta Política de Privacidade ou sobre os Dados Pessoais que são tratados pela Baluarte, entre em contato com o Encarregado de Proteção de Dados Pessoais, por algum dos canais mencionados abaixo:**tomy@baluartecapital.com** ou por correspondência para o seguinte endereço: na Rua Elvira Ferraz, 250, conjuntos 407, 408, 409 e 410, Vila Olímpia, São Paulo/SP, CEP 04552-040, aos cuidados do Diretor Sr. **Tomy Samuel Pelosof**.

8.2 A Baluarte se reserva o direito de modificar, a qualquer momento, a presente Política, especialmente para adaptá-la às eventuais alterações feitas no Sistema Baluarte. Sempre que houver uma modificação, os Titulares serão notificados acerca da mudança.

ANEXO A

PLANO DE RESPOSTA A INCIDENTES (“PRI”)

O PRI tem como objetivo estabelecer medidas de a serem tomadas pela Baluarte diante de um incidente de segurança da informação, com vistas a mitigar a ocorrência de danos causados por vazamento de dados, ataques cibernéticos, dentre outros tipos de incidentes.

1. PROCEDIMENTOS

1.1. DETECÇÃO

A primeira etapa do PRI consiste na detecção de ocorrências por meio de um gerenciamento de TI proativo.

Nesse sentido, a Baluarte realiza uma abordagem técnica, por meio de avaliação de risco, cujo intuito é identificar:

- Possíveis motivações para um ataque cibernético à Gestora; e
- Metodologias que possam ser utilizadas em ataques cibernéticos.

A Baluarte, por meio de seus protocolos e políticas internas, também realiza uma abordagem organizacional, que possibilita a detecção de incidentes cibernéticos.

1.2. RELATÓRIO DE INCIDENTE

Uma vez identificado um incidente, a Baluarte deverá produzir um relatório de acerca do incidente ocorrido (“Relatório de Incidente”), cujas informações serão utilizadas nas etapas posteriores deste protocolo.

1.3. TRIAGEM

A Baluarte realizará uma triagem do incidente ocorrido, por meio da qual será definido o grau de priorização da Gestora na mitigação de seus efeitos.

A triagem se baseará em:

- Uma avaliação inicial do incidente, com base no Relatório de Incidente;

  O nível de gravidade do incidente; e

- Impacto do incidente nos negócios da Gestora.

1.4. ANÁLISE

Uma vez realizada a triagem do incidente, a Baluarte deverá realizar uma análise de seus sistemas internos, suas redes e, a depender do caso, de *malware* de que tenha sido vítima, juntamente com a equipe de TI.

Esta etapa tem o intuito de identificar o tipo de incidente ocorrido, as informações da Gestora que tenham sido objeto de vazamento e a extensão da perda relatada, bem como a identificação das equipes e pessoas que precisam ser engajadas na solução do problema.

1.5. RESPOSTA

Como resposta ao incidente, a Baluarte atuará em três frentes:

- Contenção: definição de papéis e responsabilidades aos seus Colaboradores, conforme o caso;

- Erradicação: determinar "se" e quais sistemas da Gestora deverão ser desconectados e/ou desabilitados; e

- Recuperação: recuperar e/ou restaurar sistemas que tenham sido impactados.

1.6. ACOMPANHAMENTO PÓS-INCIDENTE

Como etapa final, a Baluarte promoverá um acompanhamento pós-incidente e atuará, de forma a:

- Analisar as medidas tomadas e sua efetividade;
- Notificar seus *stakeholders*; e
- Atuar de forma a oferecer suporte na mitigação dos danos incorridos por todos os envolvidos no incidente em questão.

ANEXO B

CARTILHA DE AVALIAÇÃO DE RISCO DE ATAQUE CIBERNÉTICO

Esta Cartilha de Avaliação de Risco de Ataque Cibernético constitui um adendo à Política de Contratação de Terceiros da Baluarte Capital Gestão de Recursos LTDA. ("Baluarte" ou "Gestora"), e tem como objetivo fornecer uma visão acerca dos parâmetros empregados pela Baluarte na detecção de ataques cibernéticos pela Gestora.

1. PREMISSAS E DEFINIÇÕES

A Baluarte atuará na detecção dos riscos de ataque cibernético por meio da identificação das principais motivações para um ataque cibernético à Gestora com base na categorização das informações digitais armazenadas por ela, utilizando como fundamento para a metodologia adotada o Guia de Cibersegurança ANBIMA, datado de dezembro de 2017. O referido documento é um dos principias materiais sobre o tema no Mercado Financeiro, incluindo as melhores referências sobre proteção de dados.

Dado que as ameaças cibernéticas podem variar de acordo com a natureza, vulnerabilidade, informações ou ativos de cada organização, os métodos utilizados por invasores mais comuns são:

- *Malware – softwares* desenvolvidos para corromper computadores e redes:

- Vírus: *software* que causa danos a máquina, rede, *softwares* e banco de dados;

- Cavalo de Troia: aparece dentro de outro *software* e cria uma porta para a invasão do computador;

- *Spyware*: *software* malicioso para coletar e monitorar o uso de informações; e

- *Ransomware*: *software* malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

- Engenharia Social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

  - *Pharming*: direciona o usuário para um site fraudulento, sem o seu conhecimento;

  - *Phishing*: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

  - *Vishing*: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

  - *Smishing*: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

  - Acesso pessoal; pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (*distributed denial of services*) e *botnets* - ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos *botnets*, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar *spam* ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (*advanced persistent threats*) - ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

2. IDENTIFICAÇÃO DE RISCOS (*RISK ASSESSMENT)*

Durante a avaliação de risco inicial, a Baluarte atuará na identificação de todos os processos e ativos relevantes da Gestora (sejam equipamentos, sejam sistemas ou dados) usados para seu correto funcionamento, levando em consideração os principais métodos utilizados por invasores, listados no item 1 acima e atuará na criação de barreiras, com a utilização de ferramentas de tecnologia e do treinamento de seus Colaboradores, como um dos passos na mitigação dos riscos de ataques cibernéticos.

Paralelamente, a Baluarte definirá quais informações são as de maior sensibilidade para a Gestora, assim como aquelas que teriam maior impacto financeiro, operacional e reputacional para si, em caso de incidente de segurança.

Assim, a Baluarte classifica as informações digitais da instituição em 3 (três) classes diferentes, quais sejam:

a) *Green Flag*:

- Quaisquer informações e/ou dados que a Gestora teve acesso ou conhecimento por ser de domínio público (“Informação Pública”);

- Quaisquer informações e/ou dados que não estejam sujeitas a compromissos ou acordos de confidencialidade; ou

- Quaisquer informações e/ou dados que tenham a obrigatoriedade de divulgação por lei ou autoridade competente.

b) *Yellow Flag*:

- Quaisquer informações que venham a ter a obrigatoriedade de divulgação por lei ou autoridade competente, mas o termo legal ainda não foi iniciado ou findado (Ex. Data de Divulgação);

c) *Red Flag*:

- Todas as Informações Confidenciais, a saber:

    - know-how, técnicas, cópias, diagramas, modelos, amostras, programas de computador, informações técnicas, financeiras, estatísticas, logísticas ou relacionadas às estratégias de investimento ou comerciais, incluindo saldos, extratos e posições de clientes e/ou das carteiras geridas pela Baluarte;

    - operações estruturadas, demais operações e seus respectivos valores, analisadas ou realizadas para as carteiras geridas pela Baluarte; e

    - estruturas, planos de ação, relação de clientes, contrapartes comerciais, fornecedores e prestadores de serviços, bem como informações estratégicas, mercadológicas ou de qualquer natureza relativas às atividades da Baluarte e/ou de seus sócios e clientes.

A partir das definições acima, a Baluarte se empenhará para manter controles, conforme o nível de criticidade das informações e dados, sendo certo de que a prioridade será escalonada na seguinte ordem de relevância: *Red Flag*, *Yellow Flag* e *Green Flag*.

3. ATUALIZAÇÕES

Versão	Motivo da Alteração	Data de Aprovação	Autor
1	Implementação	01/11/2022	Data Protection Officer