Julius Bär
Family Office

JULIUS BAER FAMILY OFFICE BRASIL GESTÃO DE PATRIMÔNIO LTDA.

Política de Cybersecurity e Segurança da Informação

Versão	Data de Atualização
1ª	Novembro/2019
2ª	Dezembro /2021

SUMÁRIO

1. APRESENTAÇÃO

A presente Política de *Cybersecurity* e Segurança da Informação ("Política") tem como objetivo descrever os processos relacionados à segurança da informação e cibernética adotados pela **Julius Baer Family Office Brasil Ltda.** ("Julius Baer Family Office") e orientar o uso e a operação de Sistemas da Informação (conforme definido abaixo) de maneira eficiente e segura na condução de suas atividades inerentes à administração de carteiras de valores mobiliários, conforme estabelecido pela Resolução da Comissão de Valores Mobiliários ("CVM") nº 21, de 25 de fevereiro de 2021 ("ICVM 21"). Este documento faz parte do compromisso da instituição em manter altos padrões de *compliance*, ética e boa conduta no decorrer de suas atividades.

A **Julius Baer Family Office** é uma entidade afiliada do grupo Julius Baer Group Ltda. ("Grupo Julius Baer"), fundado na Suíça na década de 1890 e um dos atuais líderes globais em gestão de investimentos com foco em wealth management.

A **Julius Baer Family Office** atua com autonomia funcional em relação ao Grupo Julius Baer. Igualmente, o Departamento de Compliance da **Julius Baer Family Office** ("Departamento de Compliance") dispõe de independência e autonomia, em nível local e global, para conduzir suas atividades.

As atividades da **Julius Baer Family Office** são desempenhadas com base nos *standards* éticos do Grupo Julius Baer, em observação aos manuais, políticas, regras e procedimentos do Grupo Julius Baer, conforme aplicáveis ("Políticas Globais"), além de suas próprias políticas, guias, manuais, processos, procedimentos e controles internos ("Políticas Locais").

2. ABRANGÊNCIA

Esta Política aplica-se a todos os colaboradores da **Julius Baer Family Office**, incluindo sócios, administradores, diretores, funcionários, estagiários, consultores e colaboradores temporários e demais pessoas que possuam cargo, função, posição e/ou relação de natureza societária, empregatícia, comercial, profissional, contratual ou de confiança com a **Julius Baer Family Office**, em razão da qual poderá ter ou vir a ter acesso a informações confidenciais ou informações privilegiadas de natureza financeira, técnica, comercial, estratégica, negocial ou econômica, dentre outras ("Colaboradores"). Esta Política também abrange ações e relações profissionais de Colaboradores que envolvam, notadamente, os clientes, sócios e colegas, parceiros e provedores de serviços, concorrentes, fornecedores, representantes governamentais em todos os níveis, veículos mediáticos e meios de comunicação e investidores.

O compromisso da **Julius Baer Family Office** é atender às necessidades dos clientes e cumprir as exigências e as normas estabelecidas em lei e pelos órgãos reguladores competentes. As regras de conduta devem ser adotadas por todos Colaboradores em quaisquer situações de real ou potencial conflito de interesses ou em que houver suspeita de irregularidade.

A observação desta Política deve ser feita em conjunto com as demais Políticas Locais e Políticas Globais. Em caso de dúvidas ou necessidade de aconselhamento, é imprescindível que se busque auxílio imediato junto ao Departamento de *Compliance*.

A **Julius Baer Family Office** não assume a responsabilidade por Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso a **Julius Baer Family Office** venha a ser responsabilizada ou sofra prejuízos de qualquer natureza em razão de atos ilícitos praticados por seus Colaboradores, exercerá seu direito de regresso contra os responsáveis.

3. INFORMAÇÃO RELEVANTE E SISTEMAS DA INFORMAÇÃO

É considerada "Informação Relevante" toda e qualquer informação, conteúdo ou dado que tenha valor para a **Julius Baer Family Office**, seus Colaboradores, clientes e investidores. Além do que está armazenado nos computadores, o termo Informação Relevante engloba também as informações disponíveis em relatórios, documentos, arquivos físicos, ou até mesmo quando repassada através de conversas dentro ou fora da empresa.

Portanto, a "segurança da informação" mencionada nesta Política trata-se de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que, em conjunto, formam uma proteção adequada para qualquer empresa.

São considerados "Sistemas da Informação" os sistemas de comunicações, serviços e dispositivos por meios eletrônicos utilizados para a troca e o compartilhamento de informações da **Julius Baer Family Office**, bem como os controles inerentes à tais sistemas.

Esta Política constitui um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres dos Colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos Colaboradores em relação à segurança dos recursos com os quais trabalham, além de prever o que pode ser feito e o que será considerado inaceitável com relação ao assunto.

4. PRINCÍPIOS DE *CYBERSECURITY* E SEGURANÇA DA INFORMAÇÃO

Os princípios básicos de *cybersecurity* e segurança da informação são: confidencialidade, integridade e disponibilidade das informações.

✓ Confidencialidade: Proteção da informação compartilhada contra acessos não autorizados. A ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostos, voluntária ou involuntariamente, dados restritos e que deveriam ser acessíveis apenas a um determinado grupo de usuários.

Mais informações sobre confidencialidade podem ser encontradas no Código de Ética e Conduta.

✓ Integridade: Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaças à segurança acontecem quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

✓ Disponibilidade: Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.

Além disso, como regra geral aplicável a todas as unidades operacionais da **Julius Baer Family Office**, o acesso dos usuários às informações é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação terão, de fato, esse acesso. O controle de acessos a informações confidenciais deve ser solicitado individualmente por usuário e depois autorizadas por uma função definida (por exemplo, Gerente de linha, Proprietário dos dados, Administrador de dados, Controlador) com base no respectivo conceito de propriedade dos dados.

5. ORIENTAÇÕES SOBRE *CYBERSECURITY* E SEGURANÇA DA INFORMAÇÃO

A **Julius Baer Family Office** possui políticas, processos e controles destinados à proteção e segurança das Informações Relevantes e ao uso dos Sistemas da Informação, com o objetivo de:

✓ Identificar e mensurar riscos previsíveis relacionados à segurança, confidencialidade e/ou integridade de todos os documentos contendo Informações Relevantes, bem como avaliar e, se for o caso, melhorar a eficácia das proteções já em vigor destinadas à prevenção ou mitigação de tais riscos;

✓ Prevenir que Colaboradores demitidos da **Julius Baer Family Office** tenham acesso a documentos contendo Informações Relevantes;

✓ Supervisionar os prestadores de serviço da **Julius Baer Family Office** que tenham acesso a Informações Relevantes; e

✓ Restringir acesso a dados e documentos contendo Informações Relevantes e assegurar o seu correto armazenamento e transferência.

5.1. Proteções para Cybersecurity e Segurança da Informação

Foram desenvolvidas proteções administrativas, técnicas e físicas para gerir os riscos relacionados a *cybersecurity* e segurança da informação. Essas proteções foram implementadas com base no modelo de negócios da **Julius Baer Family Office** e estão

alinhadas com as Políticas e Procedimentos Globais do Grupo Julius Baer, com a regulação aplicável e melhores práticas de *cybersecurity* e segurança da informação.

a) Propriedade de ativos relacionados a informações

Cada informação específica possui um proprietário responsável por tal ativo. Nesse contexto, a responsabilidade exige do proprietário a definição dos requisitos de segurança da informação por meio da classificação da informação em questão, de acordo com a sua sensibilidade e necessidade de sigilo e como parte da política de privacidade de dados.

b) Proteção dos ativos relacionados a informações

Medidas adequadas para proteção das informações devem considerar requisitos e restrições relacionadas aos negócios, à eficiência econômica, à legislação e à regulação aplicável.

c) Divisão de obrigações

A divisão de obrigações (*four-eye principle*) deve ser aplicada para separar responsabilidades e atribuições conflitantes. Deve ser assegurado que nenhum Colaborador possa autorizar ou implementar requisitos de mudança de acesso sem a devida aprovação do gestor da respectiva área. Ademais, para eliminar a dependência em pessoas-chave ou pontos específicos de falhas, processos e funções sensíveis nunca devem estar sob o controle de uma única pessoa.

d) Princípio *need to know*

Colaboradores somente estão autorizados a acessar informações necessárias para a execução de suas atividades. Solicitações de acesso a informações específicas devem ser autorizadas pelo gestor da respectiva área como parte do processo de segurança da informação.

e) Acesso a dados

A responsabilidade legal pelas informações é da **Julius Baer Family Office**, independentemente da forma de seu processamento e cuidado dos Colaboradores.

Este princípio também é aplicável a qualquer forma de terceirização dos serviços prestados.

O acesso ou troca de dados classificados como confidenciais ou sigilosos devem ser aprovados por um dos seguintes:

✓ respectivo proprietário das informações em caso de dados de identificação de clientes; ou
✓ o responsável pela proteção de dados em caso de informações pessoais; ou
✓ o responsável funcional e o *line manager* do Colaborador em caso de outras informações classificadas como sensíveis ou sigilosas.

f) Abordagem integrada

Controles da segurança da informação são implementados com uma abordagem integrada. Assim, tais controles não são considerados ou implementados de forma isolada, mas abrangidos como parte de uma ampla estrutura de proteção. Em situações de dificuldade para aplicar determinada divisão de cargos e posições, o monitoramento de atividades, trilhas de auditoria e/ou supervisão de risco deverão ser implementados para assegurar a devida segurança das informações.

g) Detecção e tratamento de incidentes

Existem mecanismos que garantem um alto nível de detecção e gravação de falhas de segurança da informação. Vale notar que a **Julius Baer Family Office** possui processos de reporte de incidentes e busca uma rápida reação de forma sensível e efetiva para limitar ou evitar a interrupção dos negócios.

h) Proteção e prevenção ao vazamento de dados

Mecanismos para limitar as chances de vazamento de dados devem estar instalados. Os proprietários de dados ou seus subordinados devem definir e documentar requisitos para proteção e a prevenção ao vazamento de dados. Nesse sentido, o Grupo Julius Baer possui Política Global "*D-1125-00 Global Data Protection Policy*" indicando as devidas diretrizes.

i) Sistemas de *back-up*

Sistemas de *back-up* para sistemas relevantes (como aplicativos ou infraestrutura de TI) devem ser mantidos para mitigar possíveis riscos de forma apropriada. Vale notar que a **Julius Baer Family Office** possui sistemas reservas em seu inventário para situações de contingência.

j) Ciclo de vida das informações

Medidas de segurança da informação devem cobrir o ciclo inteiro da informação. As seguintes fases devem ser cobertas:

- ✓ Criação e classificação;
- ✓ Tratamento, processamento e comunicação;
- ✓ Despacho, transporte, armazenamento e conservação; e
- ✓ Destruição.

k) Conscientização e treinamento

A **Julius Baer Family Office** possui uma cultura de conscientização sobre a segurança das informações, buscando assegurar que todos os Colaboradores estejam cientes de suas responsabilidades em relação à segurança da informação no contexto de seus cargos.

Treinamentos e orientações adequados são periodicamente disponibilizados aos Colaboradores.

l) *Compliance*

É assegurado que soluções de negócios estejam aderentes à estrutura global do Grupo Julius Baer, bem como a políticas internas locais e requisitos regulatórios aplicáveis.

5.2. Responsáveis por *Cybersecurity* e Segurança da Informação

O Comitê de Segurança de Informações é responsável pela implementação e manutenção das políticas de *cybersecurity* e segurança da informação.

O Comitê de Tecnologia da Informação é responsável pela direção geral e por fornecer os recursos necessários à execução e manutenção das políticas e procedimentos de *cybersecurity* e segurança da informação, receber atualizações periódicas da equipe de tecnologia e opinar de forma a garantir o alinhamento deste com a gestão geral de riscos da **Julius Baer Family Office** e assegurar, em conjunto com a equipe de tecnologia, que a infraestrutura da **Julius Baer Family Office** relacionada à manutenção e proteção de Informações Relevantes esteja sujeita a *backup*, redundância e resiliência no evento de um ataque cibernético (*cyber-attack*) ou outro evento que possa afetar a continuidade dos negócios.

O Comitê de Segurança de Informações reporta diretamente ao Comitê de Tecnologia da Informação. Em casos considerados necessários, os Colaboradores deverão reportar-se ao Comitê de Riscos, para que as devidas diligências possam ser tomadas, incluindo eventual reporte ao Departamento Global de Gestão de Riscos (*Global Head Risk Management*).

A equipe de Segurança da Informação ("SI") é responsável pela implementação e pelo monitoramento dos controles de segurança da **Julius Baer Family Office**. O SI define, implementa e monitora tecnologia segura e processos relacionados, dando suporte às necessidades legais, regulatórias e dos negócios, em relação à proteção da informação. Além disso, é a área que os Colaboradores devem contatar quando possuírem perguntas ou dúvidas associadas a *cybersecurity* e segurança da informação.

5.3. Procedimentos e Regras Aplicáveis às Informações de Clientes

a) Não Divulgação de Informações de Clientes

O Grupo Julius Baer tem o compromisso firme de proteger a privacidade das informações pessoais não divulgadas ao público dos seus clientes conforme definido em seus procedimentos ("Informações de Clientes") e possui procedimentos para salvaguardar registros e informações dos clientes. Informações de Clientes podem ser fornecidas a terceiros que não são coligadas do Grupo Julius Baer apenas nas circunstâncias descritas a seguir, salvo outras restrições impostas por regulamentos e leis locais:

✓ Por solicitação ou com consentimento do cliente;

✓ A terceiros conforme necessário para permitir que o Grupo Julius Baer preste serviços a clientes; e
✓ A reguladores e outros, conforme exigido ou permitido por lei.

Às vezes, as Informações de Clientes podem ser revisadas pelos prestadores de serviços externos do Grupo Julius Baer (por ex.: contadores, advogados, consultores, administradores, etc.). Esses prestadores de serviços devem manter a confidencialidade das Informações de Clientes.

É vedado aos Colaboradores, durante a vigência do contrato de trabalho ou após o desligamento do Grupo Julius Baer, divulgar as Informações de Clientes a qualquer pessoa ou entidade fora do Grupo Julius Baer, inclusive familiares, exceto nas circunstâncias descritas acima.

Um Colaborador tem a permissão de divulgar Informações de Clientes somente para outros Colaboradores ou agentes que precisam ter acesso a tais informações para entregar nossos serviços ao investidor.

A regra de confidencialidade aplica-se às informações em todos e quaisquer formatos, sejam elas obtidas de uma conversa, documentos escritos ou por outro meio. A conscientização sobre segurança da informação implica também que nenhuma informação do Grupo Julius Baer deverá ser deixada em local não seguro. Os Colaboradores são instruídos a tomar todas as medidas necessárias para proteger e preservar os documentos ou qualquer objeto de valor que esteja em seu poder contra o uso indevido, questionamento impróprio ou exposição indesejada.

b) Salvaguarda e Disponibilização de Informações de Clientes

O Grupo Julius Baer restringe o acesso às Informações de Clientes àqueles Colaboradores que precisam das informações para fornecer serviços a nossos clientes.

Qualquer Colaborador com acesso autorizado às Informações de Clientes deve guardar tais informações em compartimentos ou receptáculos seguros no encerramento do expediente, todos os dias. Todos os arquivos de computador ou eletrônicos que contenham tais informações devem estar protegidos contra acesso não autorizado. Quaisquer conversas envolvendo informações pessoais não divulgadas ao público, quando apropriado, devem ser conduzidas por Colaboradores em particular, e deve-se tomar cuidado para evitar que essas conversas sejam ouvidas por acaso ou interceptadas por pessoas autorizadas.

Qualquer Colaborador autorizado a ter a posse de “informações de relatórios de consumidores” para um propósito de negócio deve tomar medidas razoáveis para proteger-se contra o acesso não autorizado ou o uso das informações em relação à sua disponibilização.

O Grupo Julius Baer deve fornecer uma cópia destes procedimentos aos clientes no início do relacionamento entre eles e, depois, anualmente.

c) Correio eletrônico (e-mail) e outras comunicações comerciais eletrônicas

A política do Grupo Julius Baer estabelece que e-mail, mensagens instantâneas e outras comunicações eletrônicas são tratadas como comunicações por escrito e que tais comunicações devem sempre ser de natureza profissional. Nossa política abrange as comunicações eletrônicas do Grupo Julius Baer, enviadas para ou recebidas de nossos clientes e investidores, e inclui comunicações por e-mail dentro do Grupo Julius Baer.

"Comunicações comerciais eletrônicas" são comunicações de um Colaborador do Grupo Julius Baer a um terceiro na condução do negócio do Grupo Julius Baer por meios eletrônicos, tais como e-mail ou mensagens instantâneas ("MI"). Os Colaboradores do Grupo Julius Baer podem conduzir o negócio através dos seguintes formatos eletrônicos aprovados: (i) e-mail do Outlook do Grupo Julius Baer; (ii) MI do Grupo Julius Baer (apenas para uso interno); e (iii) e-mail e MI da Bloomberg. O negócio do Grupo Julius Baer não pode ser conduzido através de mensagens de texto, sites de redes sociais (por ex.: Facebook, Twitter, LinkedIn, etc.), ou contas de e-mail pessoal (por ex.: Yahoo!, Gmail, etc.). As comunicações comerciais eletrônicas que possam ser consideradas materiais de propaganda requerem aprovação do *compliance* antes da distribuição.

É importante salientar que as comunicações comerciais eletrônicas e quaisquer comunicações eletrônicas, inclusive comunicações pessoais, feitas em sistemas do Grupo Julius Baer (por ex.: e-mail do Outlook e MI do Grupo Julius Baer), são de propriedade do Grupo Julius Baer. Essas comunicações podem ser revisadas, buscadas ou apresentadas em litígios, investigações regulatórias ou iniciativas internas. Por conseguinte, os Colaboradores não devem ter nenhuma expectativa de privacidade nessas comunicações e devem fazer comunicações pessoais o mínimo possível.

O Grupo Julius Baer também introduzirá o registro de chamadas telefônicas internas e externas e, sempre que apropriado, cuidará dos seguintes temas: (i) consentimento das partes para a gravação de uma chamada telefônica; (ii) solicitação e aprovação para uso de recursos de gravação de voz; (iii) acesso a chamada telefônica gravada; (iv) armazenamento, arquivamento e transferência de chamadas telefônicas gravadas. Qualquer exceção aos temas mencionados deve ser informada imediatamente à Responsável por *Compliance* e por esta ser aprovada.

O Grupo Julius Baer deve providenciar registros ordenados de sua organização comercial e interna, inclusive todos os serviços e transações realizadas por ela. Ainda, o Grupo Julius Baer deve reter registros em um meio que permita que as informações sejam armazenadas de maneira acessível para consulta futura por qualquer autoridade competente e para satisfazer as seguintes condições:

✓ qualquer autoridade competente deve ser capaz de acessar as informações prontamente e reconstituir todos os estágios importantes do processamento de cada transação;
✓ deve ser possível verificar facilmente quaisquer correções ou outras alterações, e o conteúdo dos registros antes de tais correções e alterações; e

✓ não deve ser possível, de outro modo, manipular ou modificar os registros.

Além disso, a fim de proteger informações valiosas do Grupo Julius Baer e evitar sua remoção das instalações do Grupo Julius Baer, os Colaboradores estão expressamente proibidos de usar mídias removíveis (por ex.: CDs, DVDs, USB e similares) ou links de comunicação (por ex.: cabo, rádio, infravermelho e etc.) em qualquer computador pertencente ao Grupo Julius Baer, salvo com autorização prévia por escrito da responsável pela área de *compliance*.

6. MONITORAMENTO

Os tópicos a seguir descrevem as rotinas de monitoramento periódicas destinadas a manter e, conforme necessário, reforçar as políticas e procedimentos de *cybersecurity* e segurança da informação.

Avaliação de Riscos

Avaliações periódicas de riscos à segurança cibernética e das informações são conduzidas para mensurar adequadamente os riscos atuais. Tais procedimentos facilitam a identificação e avaliação de potenciais e previsíveis riscos à segurança, confidencialidade e/ou integridade das Informações Relevantes da **Julius Baer Family Office**, bem como a mensuração e melhoramento, quando necessário, da eficácia das medidas de proteção atualmente adotadas para mitigar tais riscos. Esses procedimentos de avaliação mensuram riscos em diversas áreas da **Julius Baer Family Office**, incluindo, mas não se limitando, a segurança da área de tecnologia da informação, rede corporativa e desenvolvimento de aplicativos. Os resultados das avaliações de risco são discutidos pelos órgãos internos adequados dentro da governança corporativa da **Julius Baer Family Office**, de forma a contribuir com a estruturação de adequados procedimentos de resposta a tais riscos e quais atividades mitigadoras devem ser adotadas no futuro para o grupo como um todo ou para aquela área específica.

Monitoramento Contínuo e Revisão da Política

A Política é monitorada pela Área de Segurança de Informações de forma contínua para assegurar seu correto funcionamento com vistas à proteção das Informações Relevantes, incluindo a prevenção a acessos não autorizados ou uso não autorizado de Informações Relevantes, além da identificação da necessidade de medidas para reforçar a eficácia ou contundência da Política, conforme necessário. Adicionalmente, a área de Segurança de Informações, em consulta ao departamento jurídico e de *compliance*, revisará o escopo da Política pelo uma vez ao ano, ou com maior frequência, se necessário, em razão de mudanças significativas ao modelo de negócios ou alterações regulatórias.

Reportes de Violação ou Vulnerabilidades à Segurança

Se algum Colaborador souber ou suspeitar de uma fragilidade à segurança da informação, acessos não autorizados ou uso não autorizado de Informações Relevantes, ou qualquer violação a esta Política, tal Colaborador deverá reportar diretamente a Área de Segurança da Informação ou ao departamento jurídico e de *compliance,* pelos seguintes meios:

- **Por e-mail**: segurancadainformacao@jbfo.com
- **Por ligação telefônica** ao Help Desk; +55 11 3089-8203 ou +55 11 3089-8221.

7. MEDIDAS DISCIPLINARES

O não cumprimento das políticas e procedimentos aqui previstos pode resultar em medidas disciplinares, as quais podem incluir demissão e, se aplicável, comunicação às autoridades regulatórias competentes. Qualquer uma das pessoas supervisionadas também pode responder pessoalmente por qualquer ato ilegal ou ilegítimo cometido durante o período em que for Colaborador do Grupo Julius Baer. Essa responsabilidade pode sujeitar a pessoa supervisionada às penalidades civis, criminais ou regulatórias. O monitoramento das políticas e procedimentos aqui estabelecidos e a aplicação das sanções aplicáveis em caso de violação de tais políticas e procedimentos serão realizados primariamente pelo Comitê de *Compliance* e, localmente, pela área responsável por *compliance* do Grupo Julius Baer, nos termos do Manual de *Compliance* do Grupo Julius Baer.

8. REVISÃO DA POLÍTICA

A presente Política será revisada pelo Comitê de Segurança de Informações, no mínimo, a cada 24 (vinte e quatro) meses, ou a qualquer momento, de ofício pelo ou mediante provocação do Departamento de *Compliance*, sempre que se observarem mudanças relevantes nas normas, regras, formato das atividades ou em qualquer outro aspecto intrínseco ao dia-a-dia da **Julius Baer Family Office**, nos termos da regulamentação aplicável.

* * *