RB Investimentos

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

1. Objetivo

Esta Política tem como objetivo estabelecer as diretrizes e princípios adotados pela RB Investimentos Distribuidora de Títulos e Valores Mobiliários Ltda. (“RB Investimentos”) para garantir a proteção da segurança cibernética, assegurando a confidencialidade, integridade, disponibilidade e resiliência das informações e dos sistemas utilizados em suas operações, em conformidade com a Resolução BCB nº 85/2021 e demais normativos aplicáveis.

A Política visa estruturar um programa de segurança cibernética robusto e proporcional à complexidade, natureza e criticidade das atividades desempenhadas pela RB Investimentos, incluindo a identificação, avaliação, mitigação, monitoramento e resposta a riscos e incidentes cibernéticos, com foco na prevenção de acessos não autorizados, perda ou comprometimento de dados e interrupções sistêmicas.

Adicionalmente, esta Política tem como escopo orientar o comportamento seguro de colaboradores, prestadores de serviço, parceiros e demais usuários dos sistemas institucionais, bem como assegurar a implementação contínua de controles técnicos, administrativos e físicos compatíveis com os níveis de risco identificados, fortalecendo a cultura organizacional de segurança da informação.

Ao instituir esta Política, a RB Investimentos reafirma seu compromisso com a proteção de dados, a continuidade dos negócios, o atendimento às exigências regulatórias e a preservação da confiança de seus clientes, parceiros e demais partes interessadas no ambiente digital.

2. Abrangência

Esta Política de Segurança Cibernética aplica-se a todos os colaboradores, prestadores de serviços, terceiros contratados, estagiários, parceiros de negócios e quaisquer indivíduos que, de forma direta ou indireta, tenham acesso a sistemas, ativos, redes, bases de dados ou informações da RB Investimentos independentemente de seu vínculo contratual ou localização geográfica.

Sua aplicação abrange todas a RB Investimentos, e ambientes operacionais — físicos ou virtuais — nos quais estejam armazenadas, processadas ou transmitidas informações institucionais, inclusive dados pessoais, dados sensíveis e demais informações consideradas relevantes ou confidenciais.

Estão incluídos no escopo desta Política todos os ativos de informação da RB Investimentos, tais como:

- Equipamentos de tecnologia (servidores, estações de trabalho, dispositivos móveis, equipamentos de rede etc.).
- Softwares, sistemas e aplicações internas e de terceiros.
- Serviços em nuvem contratados, inclusive *offshore*.
- Redes internas, VPNs e canais de comunicação institucional.

- Informações armazenadas em mídias físicas ou digitais, transitando por quaisquer meios, inclusive e-mails, plataformas de investimentos e ambientes compartilhados.

Todos os processos internos e operações que envolvam coleta, armazenamento, tratamento, acesso ou descarte de informações sensíveis estão igualmente sujeitos às diretrizes desta Política.

A adesão e cumprimento das disposições aqui previstas são obrigatórios e vinculantes, sendo condição essencial para o exercício de atividades no âmbito da RB Investimentos, com aplicação de medidas corretivas e/ou sancionatórias em caso de descumprimento.

3. Equipe de Coordenação de Segurança da Informação

A Equipe de Coordenação de Segurança da Informação ("Equipe de Coordenação") incluirá representantes das equipes de segurança de TI, jurídico e de Compliance da RB Investimentos e implementará, coordenará e manterá a Política de Segurança Cibernética e reportará periodicamente à alta administração da RB Investimentos sobre o status do programa de segurança da informação e salvaguardas da instituição para proteção de informações pessoais e outras informações relevantes.

A Equipe de Coordenação terá a supervisão geral do programa de segurança da informação e sua adoção e manutenção pelas diversas afiliadas e controladas da RB Investimentos. A Equipe de Coordenação será responsável, entre outras coisas, por:

- **Avaliação de risco:** Avaliação de riscos internos e externos para informações pessoais e outras informações relevantes.
- Políticas e procedimentos de segurança da informação. Verificar se as políticas e procedimentos de segurança da informação são desenvolvidos, distribuídos e mantidos.
- **Proteções:** Garantir que medidas de proteção administrativas, técnicas e físicas razoáveis e adequadas sejam implementadas e mantidas em toda a RB Investimentos, quando aplicável, para proteger informações pessoais e outras informações relevantes.
- **Supervisão de terceiros:** Supervisionar o acesso e/ou manutenção de qualquer prestador de serviço a informações pessoais ou outras informações relevantes em nome da RB Investimentos.
- **Resposta a incidentes:** Definição e gerenciamento de procedimentos de resposta a incidentes.
- **Treinamento de segurança:** Fornecer treinamento anual para funcionários, contratados e outros constituintes que tenham acesso a informações pessoais e outras informações relevantes sobre os requisitos desta Política, e garantir que todos os participantes da sessão de treinamento formalmente reconheçam e confirmem sua participação e compreensão do treinamento.
- **Aplicação:** Fiscalizar a aplicação das políticas e procedimentos de segurança, em colaboração com a área de recursos humanos da RB Investimentos.

- **Revisão Anual e Monitoramento:** Monitorar e testar a implementação e eficácia do programa de segurança da informação em uma base contínua, e revisar a Política e as medidas de segurança definidas neste documento ao menos anualmente, e sempre que houver uma mudança material nas práticas de negócios da RB Investimentos que possa razoavelmente envolver a segurança, confidencialidade, integridade ou disponibilidade de registros contendo informações pessoais ou outras informações relevantes.

4. Classificação de Informações

A RB Investimentos adota uma classificação rigorosa de suas informações e dados, assegurando que cada tipo de informação receba o nível adequado de proteção de acordo com sua sensibilidade e criticidade. As informações são classificadas nas seguintes categorias:

1. **Informações Públicas:** Informações que podem ser divulgadas ao público sem qualquer restrição. Exemplo: material de marketing, comunicados de imprensa.
2. **Informações Internas:** Informações destinadas ao uso interno da RB Investimentos e que não devem ser divulgadas fora da organização sem autorização. Exemplo: políticas internas, procedimentos operacionais.
3. **Informações Confidenciais:** Informações que, se divulgadas sem autorização, podem causar danos à RB Investimentos, seus clientes, ou parceiros. Exemplo: dados financeiros internos, estratégias de negócios, dados de clientes.
4. **Informações Sensíveis:** Informações de alta criticidade que requerem medidas de segurança adicionais devido ao potencial de causar danos significativos à RB Investimentos, seus clientes, ou parceiros se divulgadas. Exemplo: dados pessoais sensíveis, informações financeiras detalhadas de clientes, segredos comerciais.

Em síntese, todas as informações que transitam em seus sistemas internos e envolvem informações de clientes, são consideradas sensíveis, com nível máximo de controle e acesso a circulação. Demais informações podem ser consideradas públicas, se obtidas de fontes públicas e de amplo acesso, internas, se produzidas pelas áreas internas da RB Investimentos sem a obtenção de realizar publicação ou ampla divulgação e confidenciais, no caso de serem restritas a determinadas pessoas e áreas internas. Em todos os casos, a RB Investimentos adota controles rigorosos de acesso e revisão de permissões, com objetivo de limitar a circulação das informações a áreas e/ou pessoas não autorizadas.

As seguintes diretrizes são adotadas para assegurar a proteção adequada das informações de acordo com sua classificação:

- **Armazenamento:** Todas as informações devem ser armazenadas de forma segura, utilizando criptografia e outros mecanismos de proteção conforme necessário.

- **Acesso:** O acesso às informações é controlado com base na necessidade de conhecimento, e requer autenticação adequada.
- **Transmissão:** A transmissão de informações sensíveis deve ser feita através de canais seguros e homologados pela RB Investimentos.
- **Descarte:** Informações devem ser descartadas de forma segura, garantindo a completa destruição de dados conforme as melhores práticas e regulamentações aplicáveis.

5. Avaliação de Risco

A RB Investimentos realizará uma avaliação de risco anualmente ou sempre que houver uma mudança material nas práticas de negócios que possa envolver a segurança, confidencialidade, integridade ou disponibilidade de registros contendo informações pessoais ou outras informações relevantes.

A avaliação de risco tem como objetivo:

- Identificar riscos internos e externos razoavelmente previsíveis à segurança, confidencialidade, integridade e disponibilidade de qualquer registro contendo informações pessoais ou outras informações relevantes.
- Avaliar a probabilidade e o dano potencial causado por tais riscos.
- Avaliar a suficiência e eficácia das políticas, procedimentos e medidas de segurança em vigor para tratar e controlar tais riscos.

Após cada avaliação de risco, a RB Investimentos pode, conforme apropriado, implementar medidas de segurança administrativas, técnicas ou físicas adicionais, ou modificar as existentes, para tratar e/ou minimizar qualquer risco identificado na avaliação de risco periódica.

6. Políticas e Procedimentos de Segurança da Informação

Foram desenvolvidas e disponibilizadas políticas e procedimentos de segurança da informação de acordo com as leis e normas aplicáveis para clientes, funcionários, contratados e outras partes interessadas aplicáveis para estabelecer procedimentos relacionados a:

- Classificação de informações e práticas de manuseio para informações pessoais e outras informações relevantes, incluindo o armazenamento, acesso, descarte e transferência externa ou transporte de informações pessoais e outras informações relevantes.
- Gerenciamento de acesso de usuário, incluindo identificação e autenticação (usando senhas ou outros meios apropriados).
- Criptografia (dados em repouso, transferência de dados e e-mail).
- Uso de dispositivos móveis e outras tecnologias da RB Investimentos por funcionários e terceiros.

7. Vulnerabilidades

A RB Investimentos evita a exposição de informações a riscos por meio de seus procedimentos e gerenciamento, garantindo a segurança e mitigando vulnerabilidades. Estes procedimentos também se aplicam ao desenvolvimento de sistemas internos ou na contratação de serviços prestados ou oferecidos pela RB Investimentos.

Criptografia e gerenciamento de senhas são exemplos de barreiras dos sistemas da RB Investimentos. Os critérios de seleção, compromisso e regras de custódia responsável e mecanismos de proteção em caso de exposição estão detalhados na Política de Segurança da Informação da RB Investimentos.

A RB Investimentos realiza proativamente procedimentos adicionais de segurança, como varredura de antivírus e firewall, testes de penetração, avaliações periódicas e gerenciamento eficiente de acessos de acordo com as prerrogativas de cada negócio.

Também são realizados controles de backups diários dos dados do servidor com o objetivo de reduzir eventuais e potenciais impactos, os quais são prontamente enviados para datacenters externos, inclusive fisicamente em fitas, onde os dados ficam armazenados por cinco anos (ou prazo mais longo, se exigido pelos órgãos reguladores).

Além das informações gerais, os registros do acesso controlado a esses dados são armazenados em *logs*, garantindo a segurança e rastreabilidade dos dados. A RB Investimentos reserva-se o direito de copiar, inspecionar, apagar e exibir o conteúdo de quaisquer dados armazenados, caso seja exigido por autoridade legal.

Essas rotinas (procedimentos de *backup*, gravações, atualizações de *software*, revisão de acessos e gerenciamento de senhas) aliadas à adoção das melhores práticas da RB Investimentos visam prevenir a violação de dados.

8. Medidas de Segurança

A RB Investimentos implementou e mantém medidas de segurança administrativas, técnicas e físicas de acordo com as leis e padrões aplicáveis para proteger a segurança, confidencialidade, integridade e disponibilidade de informações pessoais ou outras informações relevantes que possui ou mantém em nome de terceiros. As medidas de segurança são adequadas ao tamanho, escopo e negócios da instituição e à quantidade de informações pessoais e outras informações relevantes que possui ou mantém.

8.1. Medidas de segurança administrativas

As medidas de segurança administrativas da RB Investimentos incluem:

- Identificação de riscos internos e externos previsíveis e avaliação se as medidas de segurança existentes controlam adequadamente os riscos identificados.
- Treinamento de funcionários nas práticas e procedimentos do programa de segurança.
- Seleção dos prestadores de serviços que sejam capazes de manter proteções adequadas e exigir que mantenham as proteções por contrato.
- Alteração do programa de segurança da informação em função de mudanças nos negócios da RB Investimentos e/ou outras circunstâncias.

8.2. Medidas de segurança técnicas

As medidas de segurança técnicas da RB Investimentos, na medida do tecnicamente viável, incluem:

- **Autenticação de usuário:** Protocolos de autenticação de usuário seguros para (1) atribuição de usuários e senhas de usuário únicos, (2) garantir que as senhas estejam em conformidade com os padrões de segurança geralmente aceitos, (3) restringir o acesso somente a contas de usuários ativos e (4) bloquear o usuário após várias tentativas malsucedidas de obter acesso.
- **Controle de acesso:** Medidas de controle de acesso seguro que restringem o acesso a registros contendo informações pessoais ou outras informações relevantes àquelas cujas funções dão origem a uma necessidade legítima de acesso a tais registros, e somente então para essa finalidade legítima relacionada ao trabalho.
- **Criptografia:** Criptografia confiável de informações pessoais e relevantes, armazenadas, processadas ou gerenciadas em serviços de computação em nuvem e correio eletrônico.
- **Monitoramento do sistema:** Monitoramento de sistema razoável para prevenção, detecção e resposta ao acesso não autorizado a informações pessoais ou outras informações relevantes ou outros ataques ou falhas do sistema.
- **Ferramentas de segurança:** *Firewalls*, atualizações de segurança e *software* de segurança, como antivírus, antimalware e outros programas de segurança da Internet, são atualizados e instalados em qualquer dispositivo que armazene ou processe informações pessoais ou outras informações relevantes.

8.3. Medidas de segurança físicas

As medidas de segurança físicas da RB Investimentos incluem:

- A implementação de medidas para proteger e restringir o acesso a locais que abrigam componentes críticos do sistema ou registros físicos contendo informações pessoais ou outras informações relevantes.
- Prevenção, detecção e resposta a intrusões físicas ou acesso não autorizado a informações pessoais ou outras informações relevantes, incluindo durante ou após a coleta, transporte ou descarte de dados.

- A eliminação ou destruição segura de registros que contenham informações pessoais ou outras informações relevantes, seja em papel ou em formato eletrônico, quando não mais para ser retidos de acordo com as leis aplicáveis ou padrões aceitos.

9. Gestão de Riscos Cibernéticos e Controles de Segurança

9.1. Identificação e Avaliação de Riscos Cibernéticos

A RB Investimentos realiza, de forma estruturada e contínua, o processo de identificação e avaliação dos riscos cibernéticos, com base em metodologias reconhecidas de gestão de riscos, adaptadas à realidade do setor financeiro e às especificidades da organização.

a) Ativos Relevantes

São considerados ativos relevantes todos os componentes que suportam os serviços críticos da instituição e que, em caso de comprometimento, poderiam causar prejuízos à confidencialidade, integridade ou disponibilidade das informações. Entre os ativos mapeados destacam-se:

- Infraestrutura de data center e servidores físicos e virtuais.
- Plataformas de negociação, liquidação, custódia e registro.
- Sistemas de gestão de cadastro de clientes.
- Aplicações desenvolvidas internamente ou por terceiros que envolvam dados pessoais ou transacionais.
- Bases de dados com informações pessoais, financeiras e estratégicas.
- Ambientes de *backup*, *disaster recovery* e alta disponibilidade.
- Recursos de autenticação, identidade digital, VPNs e *tokens* de acesso.
- *Endpoints* corporativos (*notebooks*, *smartphones*, dispositivos móveis).
- Dispositivos de rede como *switches*, *firewalls* e *access points*.

Esses ativos são periodicamente revisados pela área de Segurança da Informação, em conjunto com as áreas de negócio e Tecnologia, e mantidos atualizados em inventário centralizado e classificado por criticidade.

9.2. Análise de Vulnerabilidades e Avaliação de Impactos

A partir da identificação dos ativos relevantes, são conduzidas análises técnicas e gerenciais para detecção de vulnerabilidades internas e externas que possam impactar tais ativos. Essa avaliação considera fatores como:

- Adoção (ou ausência) de controles técnicos adequados.
- Dependência de serviços de terceiros.
- Grau de exposição à internet ou a redes públicas.
- Existência de integrações com parceiros e prestadores externos.
- Comportamento de usuários e perfil de acesso lógico.

As vulnerabilidades identificadas são avaliadas segundo critérios de probabilidade de ocorrência e potencial impacto caso concretizadas, considerando tanto o risco operacional quanto o reputacional, regulatório e financeiro.

Com base nessa análise, os riscos são classificados em níveis (baixo, médio, alto ou crítico) e tratados por meio de planos de ação com prazos, responsáveis e medidas técnicas/administrativas definidas. As decisões de aceitação, mitigação ou transferência de riscos são submetidas à Governança de Segurança da Informação e, quando necessário, à Alta Administração.

9.3. Ações de Prevenção, Proteção e Controle

A RB Investimentos implementa um arcabouço abrangente de controles preventivos, proativos e reativos voltados à proteção contra ataques cibernéticos, vazamento de dados e acessos não autorizados. Esses controles abrangem pessoas, processos e tecnologias, de forma integrada.

b) Controles Técnicos:

- Segmentação lógica de rede com zonas de segurança diferenciadas.
- *Firewall* de próxima geração com detecção de intrusão (IDS/IPS).
- Antivírus corporativo com resposta automatizada a ameaças.
- Criptografia de dados sensíveis, em repouso e em trânsito, com chaves gerenciadas.
- Bloqueio e monitoramento de dispositivos de armazenamento externos.
- Controle de acessos e segregação de funções.

c) Controles Organizacionais:

- Campanhas recorrentes de conscientização e simulações de *phishing* para todos os colaboradores.
- Política formal de gestão de vulnerabilidades, com aplicação contínua de patches e atualizações críticas.
- Auditorias internas e externas sobre práticas de segurança.
- Treinamentos específicos para áreas críticas, como TI, *compliance* e atendimento.

As ações são continuamente avaliadas, com base na evolução das ameaças e no monitoramento de indicadores de risco cibernético.

9.4. Monitoramento Contínuo e Detecção de Incidentes

A instituição mantém infraestrutura dedicada ao monitoramento em tempo real de seus ativos críticos, com foco na detecção precoce de comportamentos anômalos e potenciais incidentes de segurança.

Mecanismos adotados:

- Revisão periódica de logs de acesso, comandos executados e alterações administrativas.
- Auditorias técnicas automatizadas para verificação da conformidade com políticas e *hardening* de sistemas.
- Procedimentos definidos de escalonamento em caso de detecção de ameaça, com envolvimento das áreas de TI, Jurídico e *Compliance*.

Todos os eventos são documentados, classificados conforme gravidade e tratados conforme plano de resposta a incidentes, incluindo análise de causa raiz e ações de contenção e remediação.

10. Supervisão de Terceiros

A RB Investimentos adota procedimentos para seus fornecedores e terceiros no controle e prevenção de incidentes, obrigando-os a implantar mecanismos de segurança compatíveis com a relevância e o risco do serviço prestado.

Fornecedores e prestadores de serviços estão sujeitos a uma série de procedimentos e controles antes da contratação para assegurar sua capacidade de prevenir e remediar incidentes, com gestão de recursos, procedimentos e controles adequados e proporcionais ao risco dos serviços prestados.

Esses controles envolvem políticas, padrões rígidos de seleção, gestão e supervisão dos prestadores de serviços para assegurar a confidencialidade, integridade e disponibilidade das informações, bem como sua capacidade de gestão em eventuais incidentes.

A RB Investimentos supervisiona os meios do prestador de serviços para:

- Adotar políticas de Compliance e gestão equivalentes ao risco dos serviços prestados e aos riscos a que estão expostos.
- Cumprir a legislação e regulamentação em vigor.
- Conceder à RB Investimentos acesso a (i) dados e informações a serem processadas, armazenadas ou gerenciadas pelo provedor de serviços e (ii) relatórios elaborados por empresa de auditoria independente especializada contratada pelo prestador de serviços relacionados aos procedimentos e controles utilizados.
- Assegurar a confidencialidade, integridade e disponibilidade das informações processadas, armazenadas ou geridas pelo prestador de serviços.
- Atender aos requisitos da RB Investimentos para tal prestação de serviço.
- Prestar informações para a fiscalização dos serviços a serem prestados.
- Classificar e segregar os dados do cliente RB Investimentos por meio de controles físicos ou lógicos.
- Manter controles de acesso de alta qualidade para proteger os dados e informações dos clientes.

Os procedimentos descritos neste documento também se aplicam a provedores de serviços em nuvem no Brasil e *offshore*.

As disposições dos serviços referentes ao armazenamento, processamento ou gestão de dados *offshore* respeitarão a equivalência de severidade e padrões rígidos de regulamentação e legislação de proteção de dados, bem como a existência de acordo de cooperação para troca de informações entre o Banco Central do Brasil ("BACEN") e autoridades demais fiscalizadoras, reguladoras e autorreguladoras, garantindo a não ocorrência de danos ou constrangimento à atividade regulatória do BACEN.

11. Treinamento e Segurança

A RB Investimentos mantém um programa robusto de treinamentos periódicos voltado à promoção da segurança cibernética, abrangendo todos os funcionários, sócios e terceiros relevantes que interajam com sistemas, dados ou ativos institucionais. Esses treinamentos são essenciais para assegurar a proteção de informações pessoais e outras informações relevantes, promovendo uma cultura de vigilância e conformidade com as melhores práticas e normativos, como a Resolução BCB nº 85/2021 e a LGPD.

Os treinamentos obrigatórios são aplicáveis a todos os colaboradores, sócios e terceiros com acesso a ambientes sensíveis, incluindo prestadores de serviços e parceiros de negócios. Eles serão realizados com periodicidade mínima anual, com sessões adicionais sempre que forem identificadas novas vulnerabilidades, incidentes relevantes ou mudanças regulatórias. O conteúdo dos treinamentos é estruturado para abordar:

- Requisitos desta Política, da Política de Segurança da Informação e expectativas da RB Investimentos para o manejo seguro de dados.
- Identificação e mitigação de ameaças cibernéticas, como *phishing*, *ransomware* e engenharia social.
- Boas práticas para autenticação multifator, gerenciamento de senhas e uso seguro de dispositivos corporativos.
- Protocolos de resposta a incidentes, incluindo notificação imediata de suspeitas de violações.
- Conformidade com regulamentações aplicáveis, incluindo LGPD, normas do Banco Central do Brasil e da CVM.

Os treinamentos serão ministrados por meio de uma plataforma online dedicada, projetada para oferecer uma experiência interativa e envolvente, com módulos que incluem vídeos, simulações práticas de cenários de ataque (como tentativas de *phishing*). A plataforma garante rastreabilidade completa, registrando automaticamente a inscrição, participação, desempenho em avaliações e emissão de certificados digitais. Relatórios detalhados, com métricas como taxas de conclusão, pontuações em testes e identificação de lacunas de conhecimento, são gerados para auditorias internas e externas, assegurando conformidade e permitindo a melhoria contínua do programa.

Além dos treinamentos anuais, a RB Investimentos conduzirá campanhas regulares de conscientização, incluindo comunicados por e-mail, alertas na intranet e simulações práticas de incidentes cibernéticos, integradas ao Plano de Resposta a Incidentes. Essas simulações avaliam a capacidade de resposta dos participantes e reforçam a preparação para situações reais. A eficácia dos treinamentos será monitorada por meio de indicadores de desempenho, como redução de incidentes causados por erros humanos e adesão às políticas de segurança, com resultados reportados à Governança de Segurança da Informação.

12. Plano de Resposta a Incidentes

A RB Investimentos estabelecerá e manterá políticas e procedimentos de resposta a incidentes de segurança da informação. Tais procedimentos devem incluir análises pós-incidente de eventos e ações tomadas, e medidas para abordar de forma razoável e apropriada quaisquer vulnerabilidades identificadas e outros riscos.

Além de procedimentos proativos, a RB Investimentos possui medidas de segurança reativas contra a ocorrência de quaisquer intrusões, atuando para consertar, reparar e reportar ameaças caso se transforme em um incidente.

A área de TI é responsável pelo acesso físico às instalações de TI. As violações da segurança física ou abuso físico das instalações de TI descobertas após o evento serão relatadas diretamente a esta área.

A RB Investimentos ativará o plano de resposta a incidentes e usará a tecnologia adequada para orientar e avaliar os riscos envolvendo divulgação não autorizada de informações, interrupção das operações de um negócio, ou se o prazo de recuperação for maior que o esperado e/ou impactar os serviços prestados pela RB Investimentos.

A Equipe de Coordenação apresentará relatórios aos gestores das áreas afetadas informando, sempre que possível, a natureza da infração, as partes envolvidas, os sistemas envolvidos, detalhes e consequências do incidente, medidas para prevenir futuros acidentes e efeitos colaterais de tais medidas.

Em um cenário de incidente, os procedimentos detalhados da Política de Continuidade de Negócios serão empregados. Esses procedimentos envolvem: comandar os participantes da área e as partes afetadas a redirecionar as atividades para os locais de recuperação de desastres (“DRS”), encerramento das operações no datacenter principal, ativação da recuperação dos sistemas e recuperação de dados e, por fim, validar a qualidade dos dados recuperados no DRS.

O DRS será desativado apenas quando cesse o incidente que motivou a sua ativação, os ambientes principais passarem nos testes de qualidade e funcionalidade.

Qualquer pessoa pode informar a RB Investimentos sobre suspeitas ou incidentes que envolvam acesso ou divulgação não autorizada de informações. A área responsável poderá proceder com os mecanismos de segurança de acordo com o nível de gravidade dos incidentes relatados ou suspeitas para mitigar o impacto de qualquer incidente real ou potencial.

A RB Investimentos informará oportunamente o BACEN sobre qualquer incidente que tenha sido confirmado e considerado relevante para a operação, ou seja, que constitua uma crise.

13. Revisão Anual e Monitoramento

A RB Investimentos monitora e testa regularmente a implementação e eficácia de seu programa de segurança cibernética para garantir que ele esteja operando de forma razoavelmente calculada para impedir o acesso não autorizado ou uso de informações pessoais ou outras informações relevantes.

A RB Investimentos revisa esta política e as medidas de segurança aqui definidas pelo menos anualmente, ou sempre que houver uma mudança material nas práticas de negócios da RB Investimentos que possa envolver a segurança, confidencialidade, integridade ou disponibilidade de registros contendo informações pessoais ou outras informações relevantes.

Os mecanismos de medidas de segurança estabelecidos nesta Política serão testados anualmente para identificar suas vulnerabilidades ou de qualquer provedor de serviço, a fim de proteger os dados.

Os testes incluem análises de (i) eficácia dos controles de acesso, (ii) tecnologia de criptografia e/ou processos aplicáveis ao processo, armazenamento e gerenciamento de informações, (iii) comunicação de dados utilizados pela RB Investimentos ou seus prestadores de serviços, (iv) controles utilizados pela RB Investimentos ou seus prestadores de serviços, (v) testes de penetração, (vi) varredura de vulnerabilidade, (vii) revisão de gerenciamento de computador, (viii) treinamento do pessoal da RB Investimentos ou de sua prestadora de serviços em relação a esta Política.

14. Cultura e Disseminação

A RB Investimentos adota mecanismos para assegurar a disseminação da cultura de segurança cibernética, atendendo ao disposto na Resolução BCB nº 85/21. Para fortalecer essa cultura e garantir a segurança na utilização de seus produtos e serviços, a RB Investimentos comunica regularmente aos clientes e colaboradores as precauções necessárias por meio dos seguintes mecanismos:

- **Plataforma de Investimentos:** Informações sobre práticas de segurança cibernética e precauções no uso dos serviços são disponibilizadas diretamente no site da RB Investimentos. Os clientes têm acesso a orientações atualizadas sobre como proteger suas contas e dados, incluindo alertas sobre possíveis ameaças cibernéticas.
- **Manual do *Home Broker* (HB):** O manual do HB contém diretrizes detalhadas sobre a utilização segura da plataforma, incluindo orientações específicas sobre autenticação segura e boas práticas no uso dos serviços oferecidos pela RB Investimentos.
- **Materiais de Apoio e Comunicados:** A RB Investimentos utiliza materiais informativos, como guias, e-mails e comunicados disponibilizados nos canais internos e externos de comunicação, para prestar esclarecimentos adicionais sobre as precauções que os clientes devem adotar ao utilizar os produtos e serviços. Esses materiais são atualizados conforme necessário para refletir novas ameaças e recomendações.
- **Campanhas de Conscientização e Treinamentos:** Periodicamente, são realizadas campanhas de conscientização e treinamentos voltados aos colaboradores, abordando tópicos relacionados à segurança cibernética, como identificação de tentativas de *phishing*, importância do uso de autenticação multifator e cuidados no compartilhamento de informações pessoais.

Essas medidas têm como objetivo assegurar que todos os clientes e colaboradores estejam devidamente informados sobre as precauções necessárias na utilização dos produtos e serviços da RB Investimentos, contribuindo para um ambiente seguro e alinhado às melhores práticas do mercado e às exigências regulatórias.

15. Revisão

Esta Política deve ser revisada e aprovada pela Diretoria da RB Investimentos, sendo posteriormente compartilhada na intranet.

16. Vigência

Esta Política entra em vigor na data de sua publicação e será revisado anualmente ou sempre que houver alguma alteração na diretriz por ela estabelecida ou alterações nos requerimentos regulatórios ou de autorregulação que regem o tema.

17. Palavras-chave

Segurança, segurança cibernética, proteção de dados.

18. Documentos Corporativos Relacionados

Plano de Resposta à Incidentes e Política de Segurança da Informação.

19. Glossário

Serviços de Nuvem *Offshore* – serviço de nuvem de armazenamento de dados hospedados fora do Brasil.

Disaster Recovery Site (DRS) – local físico secundário, abriga uma estrutura de TI quase sempre idêntica à estrutura primárias, com objetivo de atender ao negócio em caráter emergencial, na falta de um serviço ou mais do site primário.

20. Registro de alterações

Versão	Item	Descrição resumida da Alteração	Motivo	Data
01	-	Criação da política	Criação	18/02/2019
02	-	Revisão	Revisão anual	01/11/2020
03	-	Revisão	Revisão anual	23/11/2021
04	-	Revisão	Revisão anual	07/03/2023
05	-	Revisão	Revisão anual	16/10/2024
06	-	Adequação a normas da ANBIMA	Revisão	14/08/2025
07	-	Atualização do tópico 11 - Treinamento e Segurança	Revisão	23/09/2025

21. Aprovadores

Alçada Responsável	Nome	Assinatura
Diretor	Adalbero de Araujo Cavalcanti	As aprovações foram realizadas através de Ata
Diretor	Glauber da Cunha Santos	As aprovações foram realizadas através de Ata
Diretor	Josil Abel Xavier da Silva	As aprovações foram realizadas através de Ata
Diretora	Marília Pimentel Garcia	As aprovações foram realizadas através de Ata
Diretor	Mauro Aparecido Gimenez Pontes	As aprovações foram realizadas através de Ata
Diretor	Mauro Tukiyama	As aprovações foram realizadas através de Ata
Diretor	Ralph Bicudo Annicchino	As aprovações foram realizadas através de Ata

22. Dúvidas

Área	Contato
Segurança da Informação	Roberto Traballi
Segurança da Informação	César Lie