RB Investimentos

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Sumário

1. Objetivo

Esta Política de Segurança da Informação tem como objetivo estabelecer as diretrizes, princípios e controles necessários para garantir a proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações da RB Investimentos Distribuidora de Títulos e Valores Mobiliários Ltda. ("RB Investimentos"), bem como dos sistemas, dados, ativos tecnológicos e demais recursos de informação sob sua responsabilidade.

A Política visa assegurar que os serviços de tecnologia da informação sejam prestados de forma segura e resiliente, prevenindo acessos não autorizados, vazamentos, perdas ou interrupções, e mitigando os impactos de potenciais incidentes de segurança, fraudes ou falhas operacionais. Tais controles aplicam-se a todas as etapas do ciclo de vida da informação, desde sua criação até seu descarte seguro.

Além disso, esta Política disciplina a concessão e o gerenciamento de acessos, o uso adequado dos recursos computacionais, a gestão de riscos tecnológicos e o comportamento esperado de todos os usuários — colaboradores, terceiros e prestadores de serviço — no tratamento de dados corporativos e pessoais, em consonância com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), a Resolução BCB nº 85/2021, o Código de Conduta e Ética da instituição e demais normativos regulatórios aplicáveis.

Ao institucionalizar esta Política, a RB Investimentos reafirma seu compromisso com a governança da informação, a proteção dos dados de seus clientes e parceiros, e a promoção de uma cultura organizacional voltada à segurança, conformidade e responsabilidade digital.

2. Diretrizes

2.1. Abrangência

Os princípios e procedimentos são válidos para toda a RB Investimentos, bem como seus colaboradores, terceiros e usuários das instalações de TI da instituição.

2.2. Avaliação de Riscos

A instituição, por meio de sua equipe de TI, realiza avaliações de risco regulares de seu ambiente de segurança da informação. O objetivo de tal avaliação é estimar a vulnerabilidade em potencial da empresa, para garantir que as medidas de segurança em uso são suficientes para reduzir os riscos a patamares aceitáveis e para estimar os investimentos associados à obtenção de nível apropriado de segurança.

Os riscos potenciais incluem:

- Usuários com nível de acesso superior ao necessário (controles de acessos inadequados).
- Terminais desligados incorretamente.
- Nomes de usuário e senhas repetidas.

- Não aderência aos procedimentos (conscientização dos colaboradores).
- Colaboradores insatisfeitos.
- Ignorância quanto aos procedimentos de segurança (conscientização dos colaboradores).
- Acesso não-autorizado necessário (controles de acessos inadequados).
- Vírus (procedimentos adequados de segurança e software antivírus).
- Falta de controle sobre mudanças feitas nos sistemas ou dados (manutenções e atualizações técnicas e de segurança dos sistemas).
- Consequências legais decorrentes de violações de segurança.
- Incêndio (continuidade de negócios).
- Inundação (continuidade de negócios).
- Sabotagem (continuidade de negócios).
- Riscos associados ao acesso à Internet (situações de ameaça externa e interna da rede).
- Dependência de poucos Colaboradores para administrar questões de segurança.

2.3. Responsabilidades

A equipe de TI é responsável pelos equipamentos que administra e por garantir a segurança das informações, cumprindo os critérios abaixo sinalizados:

- controle do acesso aos sistemas críticos.
- informes e treinamentos de conscientização de acordo com esta política.
- manutenção e atualização técnicas dos sistemas.
- descarte de dados e equipamentos de maneira segura.

De maneira geral, é responsabilidade de todos os usuários:

- Garantir a manutenção da confidencialidade, da privacidade e integridade dos dados.
- Guardar seu nome de usuário e senha de maneira segura.
- Garantir a segurança de seu terminal, desligando ou bloqueando quando não estiver em uso.
- Garantir a segurança e privacidade dos impressos produzidos.
- Estar em conformidade com as políticas, procedimentos e diretrizes da empresa.
- Ao utilizar as páginas de redes sociais e ou rede de terceiros utilizando equipamentos tecnológicos da instituição, seguir a política de Segurança da Informação tendo consciência e cuidando do sigilo em caso de compartilhamento de informações pessoais e/ou relevantes.
- Não forjar mensagens de e-mail, matérias, ou qualquer tipo de correspondência eletrônica.
- Não utilizar senha ou acesso de usuário que não seja o seu próprio, tendo em mente que a utilização de usuários de outro colaborador além de impedir a rastreabilidade das atividades, expõe a instituição a sérios riscos, dentre eles, mas não limitados, a multas devido a violação de licenças de ferramentas contratadas de terceiros.

Os gestores de equipe são responsáveis pela aderência dos membros de seus times aos princípios e procedimentos desta Política. Os Colaboradores que prestam suporte de TI e administram as instalações são responsáveis pelos procedimentos de segurança dos equipamentos de TI.

Todo usuário dos recursos de TI da instituição deve formalizar, por meio de assinatura do termo de responsabilidade, o conhecimento e concordância aos princípios e procedimentos desta Política, o qual estará disponível em sua versão mais recente na Intranet. Eventuais comunicações via informativo darão divulgação de uma nova atualização.

O conteúdo informado nesta política deve ser revisado e aprovado pela diretoria responsável pelo departamento de TI ou aprovado em ata de reunião de diretoria da instituição. A aprovação pode ser obtida por meio de comunicação via e-mail ou de documento formal.

2.4. Privacidade

Os acessos lógicos a plataformas computacionais ou equipamentos com acesso à rede, como, por exemplo, fileserver, gestão, dentre outros disponibilizados, devem ser utilizados exclusivamente para atendimento aos objetivos da instituição, ou seja, devem ser salvos no espaço lógico da instituição apenas materiais que são necessários para o exercício de sua função.

A instituição tem o direito irrestrito, independentemente de qualquer aviso prévio, notificação ou formalidade, de inspecionar quaisquer dados contidos nos equipamentos de que é proprietária, rede e sistemas de computador, a ela licenciados, para prevenir, detectar ou minimizar os impactos decorrentes do uso inadequado ou em descumprimentos às suas políticas e legislação que lhe é aplicável. Os equipamentos da instituição, bem como os dados nele desenvolvidos, são de propriedade exclusiva da mesma, portanto, passíveis de serem monitorados a qualquer tempo.

Todos dados e comunicações transmitidos por meio de, recebidos por, ou contidos nos equipamentos, rede e sistema são de propriedade da instituição, sendo-lhe facultado tomar qualquer ação que julgue conveniente, a qualquer título.

2.5. Gravação de ramais

Em atendimento à legislação e normas aplicáveis, os Colaboradores (em especial, aqueles identificados com atividades obrigatórias de ramal gravado) estão cientes do sistema de gravação telefônica e concordam e autorizam que suas ligações sejam gravadas, ouvidas e compartilhadas em monitoramentos periódicos, ou conforme necessário, independentemente de sua ciência e anuência, não lhes assistindo qualquer direito sobre o material gravado.

2.6. Segurança do Sistema de Mensagem Eletrônica

Os Colaboradores ou terceiros que utilizam o sistema de comunicações por meio de mensagem eletrônica estão sujeitos, aos seguintes requisitos de segurança:

- ***Firewall*** – *firewall* de controle de borda, para limitar o acesso de originadores de mensagens eletrônicas a servidores específicos, com configuração otimizada para tratar a troca de mensagens eletrônicas.
- ***Edge filter content*** – baseado no *firewall* de controle de borda, o filtro de conteúdo atua como defesa de primeiro nível, varrendo todas as mensagens recebidas com um filtro de conteúdo atualizado automaticamente, com regras AntiSpam, endereços de ofensores e outros recursos.
- **Bloqueio de Mensagens Anônimas** – o bloqueio é realizado pelo servidor de mensagens eletrônicas, para que todas as mensagens nas quais o originador não é identificado como válido – ou seja, associado a um servidor de mensagens eletrônicas válido – sejam automaticamente rejeitadas.
- **Ferramenta Dedicada para a proteção dos E-mails** – Ferramenta para fornecimento de filtragem de spam, detecção de phishing e antivírus de várias camadas.
- ***Junk mail filter*** – servidor de mensagens eletrônicas e Outlook, programa cliente de e-mail, conta com filtros de mensagens categorizadas como indevidas – lixo eletrônico, como propagandas etc. – as quais são automaticamente classificadas e movidas para área determinada, deixando sua classificação a critério do usuário.
- **Validação de Identidade** – o servidor de correio eletrônico é integrado ao sistema de controle de acessos da rede local (*Active Directory*), SSO (*Single Sign On*) não sendo possível seu acesso sem a devida autorização à conta de rede. O acesso às caixas postais genéricas – utilizadas para contatos externos e não pessoais – é feito através de permissão via conta de acesso à rede local.
- **Proteção antivírus** – realizada na estação de cada usuário através de sistema de combate a vírus distribuído e gerenciado de forma centralizada, com atualização automática das assinaturas de possíveis vírus.
- **Canal criptografado** – com determinados parceiros, quando acordado entre as partes, a troca de mensagens é feita via canal criptografado, com a implantação de protocolo TLS (*Transport Layer Security*), em que as mensagens são trocadas em canal criptografado com a utilização de certificados digitais X.509, garantindo a validade de remetente e destinatário, bem como a confidencialidade da mensagem.
- **Alta disponibilidade** – a infraestrutura de suporte à troca de mensagens eletrônicas conta com uma arquitetura de alta disponibilidade, em que vários servidores oferecem máxima redundância, evitando a paralisação do serviço.
- **Cópia de segurança** – diariamente é executada cópia de segurança do servidor de mensagens, e posteriormente enviada para armazenamento externo.

2.7. Plano de resposta a incidentes

A instituição vai estabelecer e gerenciar políticas e procedimentos a respeito de resposta de incidentes de segurança da informação. Tal procedimento deve incluir revisões de pós-incidentes de eventos, ações tomadas e passos para razoavelmente e apropriadamente abordar e identificar qualquer vulnerabilidade e outros riscos.

Além de procedimentos proativos, instituição tem salvaguardas reativas contra ocorrências de quaisquer intrusões, agindo para reparar e reportar ameaças no caso de se tornar um incidente.

A área de TI é responsável pelo acesso físico de instalações de TI acessíveis ao público. Violações de segurança física ou abuso físico destes recursos, descoberto após o evento, será relatado diretamente para esta área.

A instituição também ativará o plano de resposta a incidentes e usará tecnologia apropriada para orientar e avaliar riscos envolvendo divulgação não autorizada de informações, interrupção das operações de uma empresa ou se o prazo de recuperação for maior que o esperado ou afetar os serviços prestados pela instituição.

O time de coordenação também apresentará relatórios aos gerentes das áreas afetadas, informando, sempre que possível, a natureza da violação, as partes envolvidas, o sistema envolvido, detalhes e consequências do incidente, medidas para prevenir futuros acidentes e efeitos colaterais de tais medidas.

Em um cenário de incidente, os procedimentos detalhados na Política de Continuidade de Negócios também serão empregados. Esses procedimentos envolvem (i) o comando dos participantes da área e das partes afetadas para redirecionar as atividades para os locais de recuperação de desastres (“DRS”), (ii) encerramento de operações no datacenter principal, ativação da recuperação do sistema e recuperação de dados e (iii) finalmente, a reconstituição dos principais datacenters após testes para validar a qualidade dos dados recuperados no DRS. Esses mesmos procedimentos podem ser utilizados pela instituição no caso de substituição de fornecedores ou prestadores de serviços relevantes.

O DRS será desativado somente quando o incidente que ocasionou sua ativação cessar e, os testes de qualidade e funcionamento dos ambientes principais forem considerados bem-sucedidos.

Qualquer pessoa pode informar a instituição de suspeitas ou incidentes envolvendo acesso não autorizado ou divulgação de informações. A área responsável poderá prosseguir com os mecanismos de segurança de acordo com o nível de gravidade dos incidentes ou suspeitas relatadas para mitigar o impacto de qualquer incidente real ou potencial.

Quando aplicável, a instituição também poderá informar o Banco Central do Brasil, em tempo hábil, de qualquer incidente que tenha sido confirmado e considerado relevante para a operação, ou seja, aqueles que constituem uma crise.

2.8. Canal de Relacionamento com o Cliente

O Canal de Relacionamento Eletrônico do Participante com o Cliente, utilizado para consultas ou transações, deve atender, pelo menos, aos seguintes critérios:

- O site deve possuir certificado digital emitido por Autoridade Certificadora aprovada pela Infraestrutura de Chaves Públicas Brasileira, a ICP Brasil ou equivalente.
- O tráfego das seguintes informações deve ser criptografado com algoritmo de Criptografia de, no mínimo, 256 bits:
    - dados de autenticação do usuário (*login* e senha).
    - dados cadastrais.
    - dados de transações entre Participante e Cliente (Ordens e transferência de recursos).
    - dados de posições dos Clientes.
- O acesso eletrônico utilizado para transações deve possuir um segundo mecanismo de autenticação.

A RB Investimentos disponibiliza informações e orienta os Clientes sobre as práticas de segurança das informações no uso de recursos computacionais, principalmente ao que se refere a:

- **Senha** - procedimentos de composição, guarda e troca de senha.
- **Riscos** - riscos envolvidos no uso da internet e métodos de prevenção.
- **Segurança** - atualização de segurança nos computadores e segurança em computadores e dispositivos móveis.

2.9. Avaliação de Contas

Responsabilidades - A responsabilidade geral pela administração da segurança de dados é do Gestor do Departamento de Infraestrutura de TI, de modo que os procedimentos possam ser implantados e monitorados sem comprometer a segurança geral das instalações de TI da instituição.

Como parte dos procedimentos de segurança, o acesso e disponibilidade a sistemas críticos será monitorado continuamente e os registros e logs de auditoria serão armazenados por 5 (cinco) anos, ou prazo maior, se assim requerido pelas autoridades regulatórias ou legais.

Detecção e Prevenção de Uso Impróprio de Conta - A área de TI registrará tentativas de ataque cibernético aos sistemas de computadores da instituição. Conforme a avaliação do ataque e a suscetibilidade da rede, alguns sistemas e contas poderão ser desativados, a fim de tratar eventuais vulnerabilidades.

Terminais que estão ligados e inativos por certo período e que não estejam sendo utilizados para processar ou monitorar tarefas em primeiro ou segundo plano, deverão ser travados automaticamente, com liberação por meio da senha do usuário corrente ou do administrador de redes.

Administração de Senhas. Senhas são o primeiro mecanismo de defesa de muitos sistemas de computadores. A seleção cuidadosa de senhas contribui com a segurança do sistema. Os usuários são responsáveis pelo teor e pela manutenção de suas próprias senhas e pela proteção de todas as contas que possuírem. As seguintes diretrizes para o uso de senhas se aplicam:

- Tamanho mínimo de 6 caracteres.
- Alteração de senha pelo usuário no primeiro login.
- Senhas devem ser modificadas regularmente, em intervalos máximos de expiração de 90 (noventa) dias.
- As senhas são bloqueadas após 5 (cinco) tentativas falhas.
- Em caso de bloqueio da senha, o usuário deve requisitar à área de TI, mediante confirmação de identidade do usuário, o desbloqueio pelo administrador.
- As senhas possuem histórico mínimo de 6 (seis) senhas utilizadas.
- As senhas deverão ter níveis de complexidade ativados, tais como ter diversos itens na mesma senha, como letras, números, maiúsculo, minúsculo.
- As senhas devem ser armazenadas de maneira criptografada.
- Senhas deverão ser protegidas pelo usuário, de forma a evitar a visualização por terceiros;
- Senhas não deverão ser compartilhadas com outros.
- Senhas não deverão ser facilmente associadas a um usuário em particular.
- Senhas não deverão ser salvas eletronicamente em aplicativos, bloco de notas, dentre outras formas.
- O *logon* de convidados será usado somente em circunstâncias especiais e somente com aprovação específica da área de TI e gestor da área responsável pelo convidado.

Usuários que suspeitarem que sua senha esteja comprometida deverão diligenciar para providenciar a alteração da mesma. O usuário deverá relatar todos os detalhes do caso à área de TI e Compliance.

Caso as senhas não estejam de acordo com as diretrizes mencionadas acima, o usuário é avisado que não está dentro da regra de complexidade e não será permitido prosseguir com o acesso até que a senha atenda aos padrões mínimos de segurança.

O *logon* automático de terminais não é permitido, salvo nos serviços configurados nos servidores com contas de acesso dedicadas.

Gestão de acessos à rede corporativa - A gestão de acessos à rede corporativa, aos sistemas aplicativos e aos bancos de dados será concedida por meio de aprovação do gestor imediato do usuário e/ou do responsável pelo sistema.

Na contratação de novo colaborador, na alocação de terceiros, ou transferência de área, o departamento de Recursos Humanos deve solicitar ao gestor da área responsável, a aprovação de acesso à rede, sistemas aplicativos e banco de dados, conforme área de atuação.

Essas informações serão enviadas à área de TI, para concessão/habilitação dos acessos, conforme especificado pelo gestor da área e demais políticas da instituição. A área de TI só configurará o acesso após o recebimento do e-mail com a aprovação do gestor da área e liberará o acesso após o aviso formalizado pela RH, após a leitura e assinatura de todos os documentos que explicam as regras e funcionamentos de segurança da instituição.

Em casos de identificação de conflitos dos acessos aprovados pelo gestor em relação à matriz de segregação de função, o gestor de TI deverá encaminhar a solicitação à área de Controles Internos, para avaliação da concessão do acesso.

Após a avaliação da área de Controles Internos, a área de TI verificará e concederá os acessos conforme matriz de segregação de função.

A revisão dos acessos é realizada anualmente. O processo é iniciado pela área de TI, que envia um e-mail para o gestor responsável da área de negócios revisar se os acessos são devidos. O gestor retorna com as solicitações de ajustes ou confirmações dos acessos, e TI finaliza o processo enviando a lista final, após modificações.

Os casos solicitados fora dos parâmetros indicados acima serão analisados individualmente, devendo contar no mínimo com autorização da área de Controles Internos e gestor da área de negócio.

Adicionalmente, a área de Controles Internos mantém o conteúdo da matriz de acessos atualizado. Anualmente, revisa todas as configurações em busca de possíveis conflitos de acessos. A área de Controles Internos retorna a matriz com as aprovações ou desaprovações de mudanças dos acessos. Cabe à própria área de Controles Internos alinhar com o gestor da área de negócio a necessidade de acesso de determinado colaborador ou terceiro.

2.10. Arquivo e Retenção do Histórico de Acesso

O histórico de acessos dos usuários à rede interna de computadores será controlado de forma individualizada pelo recurso que detém as informações. No caso dos acessos aos dados armazenados em servidores, os eventos de segurança, registrados no servidor, servirão como evidência para os acessos.

Em relação aos acessos aos sistemas em geral, o controle e armazenamento serão realizados pelo próprio sistema operacional, gerenciado pelo controle de acesso login e logout do usuário, data e horário. Todos os históricos terão prazo de retenção compatível com as exigências legais e regulatórias.

2.11. Informações Confidenciais e Privilegiadas

A RB Investimentos considera como informações confidenciais e/ou privilegiadas todos os dados, documentos e registros, em qualquer formato (físico ou digital), que, por sua natureza, não sejam de domínio público e que, se divulgados indevidamente, possam causar prejuízos à instituição, aos seus clientes, parceiros ou demais partes interessadas.

São exemplos de informações consideradas confidenciais e/ou privilegiadas:

- Informações cadastrais, financeiras, operacionais e transacionais de clientes, investidores, fornecedores e parceiros.
- Dados pessoais e sensíveis de colaboradores e terceiros, nos termos da Lei Geral de Proteção de Dados (LGPD).
- Informações contábeis, orçamentárias e estratégicas internas.
- Documentos corporativos relacionados à estrutura organizacional, políticas, controles internos e sistemas.
- Detalhes sobre ofertas públicas de valores mobiliários, operações estruturadas, fusões, aquisições ou quaisquer eventos relevantes em estudo ou execução.
- Propriedade intelectual, algoritmos e modelos de negócios utilizados pela instituição.

As informações privilegiadas incluem, mas não se limitam a dados não públicos que possam influenciar decisões de investimento e/ou alterar o comportamento do mercado, devendo ser protegidas de acordo com a regulamentação vigente.

2.12. Preservação e Controle de Acesso às Informações Confidenciais

A RB Investimentos adota um conjunto de medidas organizacionais, técnicas e administrativas para garantir a preservação da confidencialidade, integridade e disponibilidade das informações confidenciais e privilegiadas, restringindo o seu acesso exclusivamente às pessoas autorizadas.

O processo de preservação e controle envolve:

- **Classificação da informação** quanto ao seu grau de sensibilidade (pública, interna, confidencial, restrita).
- **Definição de perfis de acesso** com base no princípio do menor privilégio e da segregação de funções.
- **Aprovação formal de acessos** por gestores responsáveis e validação pela área de Tecnologia da Informação e Controles Internos.
- **Concessão de acessos temporários** apenas quando justificado e com prazo determinado.
- **Revisões periódicas** de acessos, realizadas em conjunto pelas áreas de TI, Controles Internos e *Compliance*.
- **Revogação imediata de acessos** em casos de desligamento, afastamento ou mudança de função.
- **Registros de *logs*** para auditoria e rastreabilidade de acessos.

Todos os colaboradores, prestadores de serviço e terceiros que, por qualquer motivo, tenham acesso a informações classificadas como confidenciais ou privilegiadas, devem firmar Termo de Confidencialidade, além de serem treinados sobre os deveres de sigilo, responsabilização e consequências de vazamentos ou uso indevido.

2.13. Testes do Programa de Segurança da Informação

Com o objetivo de assegurar a eficácia e a resiliência de seus controles de segurança, a RB Investimentos realiza testes periódicos e sistemáticos de seu programa de segurança da informação, abrangendo tanto aspectos técnicos quanto procedimentais.

Entre os principais testes e avaliações realizados estão:

- **Testes de vulnerabilidade e *scans* automatizados** para identificar falhas técnicas.
- **Testes de invasão (*penetration tests*)** internos e externos, realizados anualmente por empresas especializadas.
- **Simulações de ataques cibernéticos e engenharia social**, a fim de testar a resposta dos colaboradores.
- **Testes de recuperação de desastres e restauração de *backups***, vinculados ao Plano de Continuidade de Negócios.
- **Revisões manuais e automatizadas de perfis de acesso e segregação de funções (SoD)**.

A periodicidade mínima desses testes é anual, podendo ser ajustada conforme avaliação de risco ou alterações relevantes na estrutura tecnológica da empresa. Os resultados obtidos são documentados, analisados e, quando necessário, desdobrados em planos de ação corretiva supervisionados pela área de Segurança da Informação e reportados à alta administração por meio do fórum de Riscos.

2.14. Ações de Proteção, Prevenção e Controle contra Vazamento de Informações

A RB Investimentos implementa um conjunto de ações preventivas, protetivas e reativas para mitigar os riscos de vazamento de informações confidenciais e privilegiadas, assegurando sua proteção ao longo de todo o ciclo de vida da informação.

Dentre as principais ações adotadas, destacam-se:

- **Criptografia de dados** em repouso, em trânsito e em dispositivos móveis.
- **Autenticação multifator (MFA)** para acesso a sistemas a determinados sistemas.
- **Restrição e monitoramento de uso de mídias removíveis** (ex: USBs).
- **Bloqueio automático de estações de trabalho inativas**.
- **Implantação de soluções de DLP (*Data Loss Prevention*)** para detectar e prevenir saídas não autorizadas de informações.
- **Monitoramento contínuo de *logs* e eventos** com alertas automáticos.
- **Treinamentos recorrentes de conscientização** sobre riscos cibernéticos e boas práticas de segurança.

Em caso de suspeita ou confirmação de vazamento, aplica-se imediatamente o Plano de Resposta a Incidentes de Segurança da Informação, o qual prevê:

- Contenção e mitigação do incidente.
- Comunicação aos *stakeholders* e órgãos reguladores, quando aplicável.
- Análise de causa raiz.
- Implementação de medidas corretivas.
- Registro e aprendizado organizacional

2.15. Violação da Política de Segurança

A Política exprime parte das metas e princípios de governança corporativa que devem nortear os negócios da RB Investimentos e são complementares às demais políticas.

As violações de segurança devem ser informadas à área de Compliance e demais responsáveis envolvidos para que seja devidamente investigado o ato. Assim que concluída a investigação, contendo o levantamento de informações/evidências necessárias, serão determinadas medidas corretivas, de acordo com os termos do Código de Ética da instituição.

As comunicações de desvios das diretrizes desta Política devem ser direcionadas prioritariamente aos e-mails compliance@rbinvestimentos.com e controles.internos@rbinvestimentos.com.

A RB Investimentos se preocupa em estar em plena conformidade nas suas relações negócios. Por isso, além das penalidades que são impostas pela legislação, violações desta Política podem ser punidas com medidas

disciplinares cabíveis, que podem incluir desde uma advertência, até a rescisão de contrato do colaborador ou parceiro de negócio.

2.16. Segurança Física

A área de TI é responsável pela segurança física das instalações de TI de acesso público. Sistemas de alarme poderão ser utilizados e incidentes envolvendo os mesmos serão verificados pelos encarregados de segurança.

Violações da segurança física ou abuso físico das instalações de TI serão relatadas diretamente à área de TI, caso os efeitos de um incidente sejam descobertos depois do ocorrido.

2.17. Relatório de Incidentes de Segurança

A pessoa encarregada de fazer a investigação técnica de uma violação de segurança deverá apresentar um relatório ao gestor da área de TI ou pessoa designada, contendo os seguintes detalhes (se possível):

- A natureza da violação de segurança.
- A classificação geral das pessoas envolvidas no incidente (por exemplo, “cliente externo” ou “Usuário Privilegiado”).
- Os sistemas de computadores envolvidos no incidente.
- Os detalhes do incidente.
- As consequências do incidente.
- Possíveis medidas para prevenir que o incidente se repita.
- Efeitos colaterais de tais medidas.

Quando apropriado, ação remediadora deverá ser tomada com base no relatório.

2.18. Auditoria de Segurança

Procedimentos de auditoria serão realizados regularmente em todos os sistemas de computadores, para verificar se a política de segurança está sendo observada e para satisfazer as diretrizes e requerimentos previstos nas atividades de Controles Internos e Auditoria Interna e Riscos Operacionais da instituição.

Procedimentos de auditoria, em qualquer nível, podem ser realizados em qualquer instalação de TI, a critério da instituição.

Cópias de todos os registros de acesso deverão ser arquivadas em ambiente de armazenamento externo, contratado com prestador de serviço, por pelo menos 5 (cinco) anos.

2.19. Treinamento

A eficácia do programa de segurança da informação da RB Investimentos depende diretamente do engajamento, conscientização e cooperação de todos os colaboradores, sócios, terceiros e, quando aplicável, clientes, no cumprimento das diretrizes de segurança.

Os colaboradores com acesso aos sistemas de computadores são responsáveis pela proteção dos dados em suas estações de trabalho e devem seguir rigorosamente as orientações de segurança divulgadas pela instituição. Essas diretrizes visam garantir a confidencialidade, integridade e disponibilidade das informações, bem como mitigar riscos operacionais e cibernéticos.

As diretrizes de conscientização em Segurança da Informação e Tecnologia da Informação incluem:

- Esclarecer as responsabilidades e os procedimentos específicos de cada colaborador, sócio e terceiro, conforme aplicável.
- Orientar e supervisionar o uso adequado e os limites de acesso aos sistemas e recursos institucionais.
- Reforçar o entendimento das obrigações de confidencialidade e proteção de dados, conforme normativos aplicáveis, como a Lei Geral de Proteção de Dados (LGPD) e a Resolução BCB nº 85/2021.

Os aspectos de segurança da informação, incluindo confidencialidade, integridade e disponibilidade, são integrados ao processo de *onboarding* de novos colaboradores, sócios e terceiros, sendo reforçados regularmente por meio de treinamentos obrigatórios. Esses treinamentos são aplicáveis a todos os funcionários, sócios e terceiros relevantes (como prestadores de serviços com acesso a sistemas ou dados sensíveis) e têm periodicidade mínima anual, com possibilidade de realização adicional em casos de identificação de novos riscos, atualizações regulatórias ou incidentes significativos.

Os treinamentos serão ministrados por meio de uma plataforma online dedicada, que oferece módulos interativos, incluindo vídeos, estudos de caso, simulações de ataques cibernéticos (como *phishing*). A plataforma registra automaticamente a participação, progresso, resultados de avaliações e emissão de certificados digitais, garantindo rastreabilidade completa por meio de logs auditáveis e relatórios de conformidade. Esses relatórios incluem métricas como taxa de conclusão, desempenho em testes e identificação de lacunas de conhecimento, permitindo ajustes contínuos no programa de treinamento.

O conteúdo dos treinamentos abrange, mas não se limita a:
Boas práticas para gestão de senhas e autenticação segura.

- Identificação e prevenção de ameaças cibernéticas, como *phishing*, malware e engenharia social.
- Procedimentos para proteção de dados pessoais e sensíveis, em conformidade com a LGPD.
- Diretrizes para uso seguro de dispositivos corporativos e pessoais no acesso a sistemas institucionais.
- Protocolos de resposta a incidentes, incluindo a notificação imediata de suspeitas de violações.

Para novos colaboradores, sócios ou terceiros, o acesso aos sistemas institucionais será liberado somente após a conclusão do treinamento inicial de integração, que inclui a assinatura de um Termo de Compromisso e Confidencialidade, confirmando a ciência e adesão às políticas da instituição. Além disso, a RB Investimentos promoverá campanhas de conscientização contínua, com comunicados regulares, alertas sobre novas ameaças e atualizações nas diretrizes. Essas iniciativas visam fortalecer a cultura organizacional de segurança, garantindo que todos os envolvidos estejam preparados para proteger os ativos de informação e contribuir para a resiliência da instituição frente a riscos cibernéticos.

2.20. Diretrizes de Segurança para os Computadores da instituição

O Departamento de TI será responsável pela criação, manutenção e publicação de diretrizes de configurações, com o intuito de aperfeiçoar a segurança de todos os sistemas em funcionamento aprovados pelo gestor de TI.

O Departamento de TI também disponibilizará essas configurações a fornecedores aprovados, se necessário, e solicitará que tais configurações sejam utilizadas em todos os computadores entregues à instituição.

2.21. Responsabilidades Legais

Todos os usuários das instalações e serviços de TI da instituição estão sujeitos à regulamentação e leis locais e internacionais. Pessoas que violarem tais leis poderão ser sujeitas a medidas disciplinares, inclusive rescisão de contrato por justa causa, e ser intimadas a responder em processos cíveis, administrativos e criminais, conforme a extensão da violação praticada. Caso existam dúvidas sobre a legalidade de determinada conduta ou ação relacionada ao uso de equipamentos e informações de TI, o usuário deve entrar em contato com a equipe de TI e departamento de Compliance antes de proceder.

Em caso de descumprimento comprovado, ou suspeita de descumprimento da presente política, pelo Colaborador ou terceiro, o Gestor da área, departamento de RH e Compliance deverão ser envolvidos para a apuração do incidente e a tomada das medidas cabíveis.

2.22. Segurança no Desenvolvimento e Aquisição de Sistemas de Aplicação

Os processos de aquisição, desenvolvimento e manutenção dos sistemas de informação devem seguir (a) metodologia formal, a partir de uma análise crítica, que contemple aspectos relacionados às exigências legais vigentes e de segurança da informação e, (b) processo de gestão de configuração e mudança, de acordo com a Política de Gerenciamento de Mudança, de forma a garantir o controle efetivo de modificações realizadas em ambientes diversos, com o objetivo de registrar, avaliar e autorizar qualquer modificação em sistemas de informação.

Os ambientes produtivos devem ser segregados dos demais ambientes e com acesso somente via aplicação por usuários previamente autorizados ou por ferramentas homologadas.

Será obrigatória a assinatura de Termo de Compromisso ou Acordo de Confidencialidade por parte dos prestadores de serviços, contendo declarações que permitam aferir que os mesmos tomaram ciência das normas de segurança vigentes da RB Investimentos, garantindo que os dados disponíveis na aplicação só possam ser acessados pelos usuários autorizados.

3. Cultura e disseminação

A RB Investimentos se empenha para aderência aos requerimentos regulatórios e as diretrizes desta política, de forma a disponibilizar orientações sobre a estrutura e procedimentos de gerenciamento de mudanças.
A Política deve ser revisada e aprovada pela Diretoria da RB Investimentos e deve ser compartilhada na intranet.

4. 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.

5. Palavras-chave

Segurança, confidencialidade, acessos, identificação.

6. Documentos corporativos relacionados

Plano de Resposta a Incidentes e Política de Gerenciamento de Mudança.

7. Registro de alterações

Versão	Item	Descrição resumida da Alteração	Motivo	Data
01	-	Criação da política	Criação	19/04/2010
02	-	Atualizações	Revisão	26/08/2011
03	-	Revisão do conteúdo para atendimento ao PQO – B3 e mudança de Template	Revisão	
04	-	Inclusão de diretório independente da Custódia	Revisão anual	05/05/2014
05	-	Inclusão Segurança dos E-mails, Contatos Clientes e Inclusão de diretório independente da DTVM	Revisão	23/05/2014
06	-	Alteração	Revisão	15/06/2016
07	-	Proprietários para gestão (G:)	Revisão	27/06/2017

08	-	Alteração de Responsáveis, Gestão de acessos à rede corporativa e Revisão de sistemas e áreas	Revisão	14/06/2018
09	-	Revisão geral de conteúdo, conforme nova política de gravação de ligações e rotinas requeridas pela BSM, ao longo da última auditoria operacional e LGPD	Revisão anual	25/02/2019
10	-	Atualização anual	Revisão anual	29/09/2020
11	-	Revisão anual e atualização de parâmetros de senha, conforme PQO	Revisão anual	23/11/2021
12	-	Revisão anual	Revisão anual	26/01/2023
13	-	Revisão anual	Revisão anual	11/03/2025
14	-	Adequação a normas da ANBIMA	Revisão	25/07/2025
15	-	Atualização do tópico 2.19 - Treinamento	Revisão	23/09/2025

8. 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

9. Dúvidas

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