Sumário

1. INTRODUÇÃO

Esta Política de Segurança Cibernética ("Política") tem por objetivo assegurar a confidencialidade, a integridade e a disponibilidade de dados e sistemas de informações utilizados pela Ativos, na prestação de seus serviços e execução de suas atividades, bem como definir medidas e procedimentos de forma a garantir a seus clientes a devida proteção de seus dados e das transações realizadas.

2. OBJETIVO

Esta Política tem por objetivo estabelecer e comunicar os princípios, valores, conceitos, procedimentos e controles que são adotados na prestação de serviços da Ativos a seus Clientes, visando assegurar a confidencialidade, a integridade e a disponibilidade dos Dados e dos sistemas de informação utilizados, para a continuidade dos serviços prestados.

Ainda, esta Política visa viabilizar a identificação de possíveis violações de segurança cibernética, por meio da definição de ações sistemáticas de detecção, tratamento e prevenção de Incidentes, ameaças e vulnerabilidades nos ambientes físicos e digitais, a fim de mitigar, assim, os Riscos Cibernéticos, garantindo, ainda, a continuidade de seus negócios, protegendo os processos críticos de interrupções causadas por falhas ou desastres.

Por fim, esta Política tem por propósito estabelecer e melhorar o processo de Gestão de Riscos de Segurança Cibernética utilizado pela Ativos.

3. DIRETRIZ

A presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio da Ativos, bem como a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição, além da sensibilidade dos dados e das informações sob responsabilidade da Ativos.

4. DEFINIÇÕES

Clientes	Pessoas jurídicas contratantes dos serviços prestados pela Ativos.
Colaboradores	São os administradores, corpo diretivo, funcionários, jovens aprendizes, estagiários, auxiliares ou quaisquer outros colaboradores da Ativos.

Dado(s) e/ou Informação(ões)	São todos os dados referentes às atividades desenvolvidas pela Ativos na execução de seu objeto social, incluindo dados de Clientes, pessoais ou não, e classificados de acordo com o item 7 desta Política. Entenda-se por dados pessoais qualquer informação relacionada a pessoa natural identificada ou identificável.
Incidentes	Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena ou transmite ou que constitui uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis.
Prestador de Serviço	Pessoa física ou jurídica, devidamente contratada pela Ativos, prestadora de serviços: (i) de tecnologia; (ii) de armazenamento ou qualquer forma de tratamento de Dados e Informações; ou (iii) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.
Riscos Cibernéticos	São os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor Dados, redes e sistemas da Ativos, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da Ativos.

5. ABRANGÊNCIA

Os procedimentos abaixo descritos são direcionados a todos os Colaboradores e Prestadores de Serviços da Ativos.

6. REFERÊNCIAS

- Política de Segurança da Informação

7. CLASSIFICAÇÃO DE DADOS

Os Dados objeto da presente Política serão classificados de acordo com as categorias a baixo indicadas, considerando a relevância das informações e conforme Política de Uso da Informação da Ativos:

I. **Nível 01 - Documentos Públicos** – Informações aprovadas pela diretoria para uso público (interno e externo), por exemplo: relatórios anuais, indicações para a imprensa;

II. **Nível 02 – Dados Pessoais** – Informações relacionadas a uma pessoa natural, capaz de identificar um indivíduo diretamente ou de maneira indireta por meio da associação com demais informações.

III. **Nível 03 - Somente Uso Interno** – Informação não aprovada para circulação fora da Ativos como, por exemplo: memorandos internos, minutas ou atas de reuniões, procedimentos, rotinas operacionais e relatórios de projetos internos;

IV. **Nível 04 - Confidencial** – Informações cuja circulação interna é controlada, por questões estratégicas e de gestão e cuja a circulação externa é vedada, pois se tornadas públicas ou compartilhadas causarão impacto e prejuízos aos negócios, podendo ser: planos de projetos, plantas e especificações que definem a forma que a organização opera, informações contábeis, planos de negócio, informações sobre clientes ou acionistas, entre outros. Este nível envolve todas as Informações e Dados referentes aos Clientes da Ativos inclusive dados pessoais.

V. **Nível 05 - Informações Sensíveis** - Informações internas ou confidenciais críticas ao desenvolvimento das atividades da Ativos, que: (i) são acobertadas por sigilo bancário, nos termos da legislação aplicável; e/ou (ii) cuja perda ou indisponibilidade pode prejudicar ou impedir a adequada prestação de serviços pela Ativos ao Cliente, a realização de operações da Ativos e/ou o cumprimento de suas obrigações legais e/ou normativas.

A Ativos manterá um programa de revisão e de classificação contínua das informações.

8. PRÍNCIPIOS

A Ativos sempre empreenderá os melhores esforços a fim de garantir aos seus Clientes a segurança de seus Dados, bem como a qualidade e continuidade dos serviços prestados. Para tal, suas práticas são orientadas de acordo com os princípios indicados a seguir:

I. Confidencialidade: é a proteção dos Dados e Informações contra acessos não autorizados;
II. Integridade: salvaguarda da exatidão e completeza dos Dados, Informações, sistemas e serviços;
III. Disponibilidade: é a garantia de que os Dados e sistemas estarão acessíveis e disponíveis, de modo a garantir a continuidade das atividades da Ativos e o atendimento ao Cliente;

IV. Acesso Controlado: o acesso aos Dados é restrito e controlado, significando que somente os Colaboradores ou Prestadores de Serviços que devem justificadamente ter acesso a uma determinada informação, tenham referido acesso.

9. DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA

A presente Política deverá ser cumprida e respeitada por todos os Colaboradores e Prestadores de Serviços da Ativos. Neste sentido, deverão ser respeitadas as seguintes diretrizes gerais:

I. Resguardar a proteção dos Dados contra acessos indevidos, bem como contra modificações, destruições ou divulgações não autorizadas, respeitando as regras estabelecidas pelas a Política de Segurança da Informação e a Política de Uso da Informação da Ativos;

II. Realizar a adequada classificação dos Dados, conforme os critérios e princípios indicados nesta Política;

III. Garantir que os sistemas e Dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;

IV. Garantir a continuidade do processamento das informações Sensíveis, respeitadas as condições estabelecidas na Política de Continuidade de Negócios;

V. Zelar pela integridade da infraestrutura tecnológica na qual são armazenados, processados ou de qualquer outra forma tratados os Dados, adotando as medidas necessárias para prevenir ameaças lógicas, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados a Dados internos e confidencias, por meio, dentre outros aspectos:

a) da manutenção de softwares antivírus e firewall instalados e atualizados;
b) da manutenção dos programas de computador instalados no ambiente atualizados em sua última versão;
c) da realização de alteração periódica de senhas, respeitados os requisitos de segurança da Política de Gestão de Acessos a Redes e Sistemas.

VI. Atender às leis e normas que regulamentam as atividades da Ativos;

VII. Comunicar imediatamente quaisquer descumprimentos à esta Política, bem como suspeita de intrusão no sistema, infraestrutura ou no acesso aos Dados, através do e-mail protecaodados.compliance@rodobens.com.br, sob a responsabilidade da área Compliance.

VIII. O Comitê de Proteção de Dados é um organismo consultivo e colaborativo, constituído por equipe multidisciplinar, com o objetivo de auxiliar na governança em privacidade e

proteção de dados pessoais.

10. MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES

Além das diretrizes gerais supramencionadas, a Ativos informa que as seguintes medidas de segurança e controles devem ser aplicadas a fim de reduzir a vulnerabilidade a incidentes de segurança e garantir maior segurança aos Dados, aos ambientes lógicos e à continuidade de seus negócios e do atendimento ao Cliente, com foco na prevenção de Incidentes:

I. O Colaborador e os Prestadores de Serviços somente deverão possuir acesso aos Dados e Informações internos ou confidenciais após a realização de sua autenticação no sistema da Ativos, por meio de seu login, com inserção de sua senha pessoal eintransferível;

II. Na hipótese de o Prestador de Serviços não possuir, em decorrência do Contrato, acesso ao ambiente da Ativos, quaisquer Informações internas ou confidenciais, Sensíveis ou não, somente poderão ser compartilhadas: (i) na estrita medida necessária para a execução do objeto do contrato; (ii) apenas após a assinatura do contrato contendo cláusula de confidencialidade ou após a assinatura de termo de confidencialidade específico; e (iii) por meio de conexão privada e segura;

III. Informações confidenciais e/ou Sensíveis somente deverão ser compartilhadas com o Prestador de serviços de forma criptografada, protegidas por senha;

IV. Informações Sensíveis somente devem ser compartilhadas com Prestadores de Serviço mediante previsão contratual específica, devendo ser armazenadas apenas durante o período pelo qual estas sejam necessárias à execução dos serviços contratados;

V. O acesso a informações Sensíveis deve poder ser rastreado por meio da manutenção de inventário de detalhado dos registros de acesso a referidas informações, contendo o momento, a duração, a identidade do responsável e o arquivo acessado;

VI. O tratamento de dados pessoais, conforme definição trazida nesta política, deverá observar as disposições trazidas pela política empresarial de proteção de dados pessoais, disponível para consulta na Intranet.

VII. Todos os Colaboradores e Prestadores de Serviço que podem vir a ter acesso aos Dados e Informações devem assinar, obrigatoriamente, termo de confidencialidade ou possuir

cláusula de confidencialidade em seus contratos, devidamente validada pelo departamento jurídico;

VIII. Os Dados confidenciais devem ser armazenados de forma criptografada;

IX. São realizados testes e varreduras para detecção de vulnerabilidades na infraestrutura da Ativos, visando a prevenção a intrusões e ao vazamento de informações, devendo a grade de planejamento de testes ser definida pela área de Segurança da Informação, que definirá, também, a periodicidade para realização de tais testes;

X. A Ativos possui mecanismos e exige os mesmos de seus Prestadores de Serviços para localização dos Dados e Informações, assim como a identificação de como e para quais finalidades estes Dados são utilizados e quem teve acesso aos mesmos, inclusive para permitir o controle da exclusão de Informações;

XI. Todos os Dados e Informações devem possuir cópia de segurança, armazenadas conforme Política de Backup da Ativos;

XII. Deverão ser realizados treinamentos e avaliações para a devida conscientização, educação e treinamento dos Colaboradores e Prestadores de Serviços, a fim de que esta Política seja plenamente aplicada, garantindo assim a proteção e confidencialidade dos Dados e Informações e a continuidade do negócio;

XIII. Periodicamente a Ativos encaminha aos seus Clientes informações acerca das medidas de segurança essenciais à utilização de seus serviços, visando mitigar Riscos Cibernéticos.

Todas as medidas indicadas nesta Política devem ser aplicadas também na adoção de novas tecnologias, na contratação de novos serviços e no desenvolvimento de sistemas de informação pela Ativos, bem como pelos prestadores de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Ativos.

11. ESTRUTURA DE GERENCIAMENTO

Os acessos aos Dados serão devidamente controlados, monitorados, restringidos a menor permissão e privilégios possíveis, inclusive em cumprimento ao princípio de Acesso Controlado, conforme definido pela Política de Elegibilidade.

Mencionados acessos serão revistos periodicamente e cancelados tempestivamente ao término do contrato do Colaborador ou do Prestador de Serviço, conforme definido pela Política de Gestão de Identidades e Acessos.

O acesso a infraestrutura física na qual estão armazenados referidos dados seguirão as mesmas diretrizes constantes acima.

A Ativos prioriza a conscientização da importância da Segurança Cibernética a seus Colaboradores e Prestadores de Serviços. Assim, com o intuito de disseminar a cultura de segurança cibernética na Ativoss:

(i) são realizados periodicamente treinamentos e campanhas voltados aos Colaboradores e Prestadores de Serviços, incluindo avaliação de pessoal;

(ii) e (ii) são fornecidas informações a Clientes e usuários sobre precauções na utilização de produtos e serviços financeiros da Ativos. A Ativos manterá programas de capacitação e de avaliação periódica de pessoal referentes a esta Política.

Os procedimentos devem ser estabelecidos para assegurar que os controles sejam executados dentro dos parâmetros estabelecidos e monitorados quanto a sua efetividade diante das mudanças tecnológicas e do contexto do negócio. Através de registros e verificações periódicas serão geradas as evidências de atendimento aos parâmetros estabelecidos.

As mudanças nos acessos serão documentadas através de solicitações previamente aprovadas de acordo com alçadas e responsabilidades para garantir que o acesso é devido e de acordo com as necessidades para os cumprimentos das funções e objetivos do negócio.

12. CONTINUIDADE DE NEGÓCIOS

O processo de gestão de continuidade de negócios relativo a segurança da informação, é implementado para minimizar os impactos e recuperar perdas de ativos da informação, após um incidente crítico, retornando a operação a um nível aceitável, através da combinação de requisitos como operações, funcionários chaves, mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.

Referido processo seguirá o quanto estabelecido na Política de Continuidade de Negócios da Ativos e deverá considerar, ao menos, os seguintes cenários para a realização de testes de continuidade de negócios:

I. Exploração de possíveis vulnerabilidades que permitam o acesso, a cópia e /ou a extração de Informações e Dados internos e/ou confidenciais do ambiente lógico da Ativos;

II. Realização de testes de intrusão a base de dados contendo Informações Sensíveis da Ativos;
III. Tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;
IV. Estratégias para a recuperação de Informações Sensíveis e Serviços Relevantes.

Referidos testes devem respeitar as condições definidas pela Política de Continuidade de Negócios da Ativos.

13. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES

As Empresas Rodobens, cujas atividades exploradas são reguladas pelo Banco Central do Brasil, disponibilizará as informações sobre os seus incidentes relevantes, em especial, seus registros, analises da causa e do impacto e os controles dos efeitos dos incidentes com as demais instituições financeiras e autorizadas a funcionar pelo Banco Central do Brasil por meio das iniciativas ajustadas entre as instituições, resguardando o sigilo bancário das informações, seus segredos de negócios e privilegiando a livre concorrência entre os participantes do mercado.

14. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

A contratação de **serviços relevantes** de processamento, armazenamento de dados e de computação em nuvem esta sujeita ás condições previstas nesta Política.

São considerados **serviços relevantes,** isoladamente ou cumulados:

I. **Quanto a criticidade dos serviços:** serviços essenciais para operação da organização, atendimento ao público e aqueles que podem impactar na continuidade do negócio;
II. **Quanto à sensibilidade dos dados e inforamações:** serviços envolvendo **alto volume de informações** sobre clientes, colaboradores, parceiros e/ou fornecedores em geral. Entende-se por **"alto volume de informações"** o envolvimento de mais de 1.000 (um mil) cadastros de clientes, colaboradores, parceiros e/ou fornecedores em geral.

A contratação de serviços relevantes deverá ser precedida das seguintes providências:

I. Avaliar a maturidade do fornecedor em segurança da informação, sob a responsabilidade da área Tecnologia da Informação;
II. Avaliar a maturidade do fornecedor em relação à Lei 13.709/2018 (Lei Geral de Proteção de Dados), sob a reponsabilidade da área Compliance;
III. Formalizar contrato, sob a responsabilidade da área Jurídico Consultivo.

A contratação de fornecedores para prestar serviços relevantes será precedida de aprovação da gerência geral da área Tecnologia da Informação e, se envolver dados pessoais, da gerência geral da área Compliance. Existindo riscos, a operação deverá ser aprovada pela administração da organização, conforme alçadas definidas na Política de Contratos.

Compliance comunicará ao Banco Central do Brasil a contratação de serviço relevante, no prazo de 10 (dez) dias, contado da data de conclusão do processo de assinatura do contrato.

Ainda, caso os serviços, ou parte deles, sejam prestados no exterior, deverão, as autoridades supervisoras dos países onde estes serão prestados, possuir convênio de troca de informações com o Banco Central do Brasil. Em hipótese de inexistência do supramencionado convênio, Compliance deverá solicitar autorização do Banco Central do Brasil para tal contratação, no prazo de 60 (sessenta) dias antes da contratação.

Referida solicitação também será necessária caso, durante a execução do contrato, alterar as seguintes condições: fornecedor, serviço relevante contratado e/ou os países e regiões onde os serviços poderão ser prestados.

RESPONSABILIDADE

O corpo diretivo da Ativos se compromete com a melhoria contínua dos procedimentos e controles relacionados nesta Política, os quais devem ser objetos de pautas recorrentes em Comitês internos da empresa.

15. RESPONSABILIDADES GERAIS

É dever de todos os colaboradores, ter acesso e entender o presente documento, bem como saber das suas respectivas obrigações em relação a sua aplicação.

Cabe aos supervisores e coordenadores da área, observar e garantir o cumprimento das diretrizes aqui descritas, bem como avaliar e efetuar a atualização do conteúdo quando necessário.

As situações de não conformidade com esta Política deverão ser imediatamente reportadas ou comunicadas ao Gerente e/ou Superintendente, o qual caberá dar o tratamento adequado aos casos que lhe forem reportados.

16. DISPOSIÇÕES GERAIS

Esta Política é disponibilizada a todos os colaboradores da organização, através da Intranet, para conhecimento e cumprimento das diretrizes necessárias para a gestão de Compliance.

Esta Política está sujeita a revisões a cada dois anos, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável

ou, ainda, para refletir alterações nos procedimentos internos das Empresas Rodobens.

17. PENALIDADES

O cumprimento de todas os documentos publicados é exigido de todos os Colaboradores da Companhia constituindo-se em violação a não observância aos preceitos nelas descritos, podendo acarretar a aplicação de medidas disciplinares conforme o código de ética.

18. COMUNICAÇÃO

Em caso de dúvidas acerca desta Política, contate a área Compliance pelo e-mail protecaodados.compliance@rodobens.com.br.

19. QUADRO DE REVISÃO

Controle de Revisões:			
Revisão	**Data**	**Área**	**Motivo da Revisão**
4	29/06/2023	Compliance	Revisão do documento

ANEXO I – MODELO DE TERMO DE ADESÃO

TERMO DE ADESÃO A POLÍTICA DE SEGURANÇA CIBERNÉTICA DA ATIVOS ADMINISTRAÇÃO DE CARTEIRA DE VALORES MOBILIÁRIOS LTDA

Eu, [nome], [qualificação], declaro que tomei conhecimento dos termos e condições da Política de Segurança da Cibernética da Ativos – Administração De Carteira De Valores Mobiliários Ltda. ("Política" e "Ativos"), por meio de treinamento realizado em [●] de [●] de [●] na sede da Ativos, tendo, ao final, recebido uma cópia do Manual. Subscrevendo o presente formalizo a minha adesão ao presente Manual, comprometendo-me a cumprir com todos os seus termos e condições, adotando, nas situações de dúvida, a posição mais conservadora possível, submetendo as dúvidas a respeito do cumprimento do Manual e da legislação e regulamentação em vigor ao Diretor responsável pelo Compliance.

Barueri, [●] de [●] de [●].

_____
[●]

Testemunhas:

1. _____ 2. _____
Nome: Nome:
RG: RG:
CPF: CPF: