Esta Política de Segurança Cibernética (“Política”) tem por objetivo assegurar a confidencialidade, a integridade e a disponibilidade de dados e sistemas de informações utilizados pelas Empresas Rodobens, 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.

ÍNDICE

1. DEFINIÇÕES 1
2. BASES DA POLÍTICA 3
3. OBJETIVO DA POLÍTICA 3
4. ABRANGÊNCIA 3
5. DOCUMENTOS REFERENCIADOS 3
6. CLASSIFICAÇÃO DE DADOS 4
7. PRÍNCIPIOS 5
8. DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA 5
9. MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES 6
10. INCIDENTES DE SEGURANÇA 7
11. ESTRUTURA DE GERENCIAMENTO 9
12. CONTINUIDADE DE NEGÓCIOS 10
13. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES 11
14. PROCESSAMENTO, ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM 11
15. GUARDA DE DOCUMENTOS 12
16. RESPONSABILIDADE 12
17. COMUNICAÇÃO 12
18. PENALIDADES 13

1. DEFINIÇÕES

1.1 Para devida compreensão e aplicabilidade desta Política, são consideradas as definições indicadas a seguir:

a) **Clientes:** pessoas físicas e/ou jurídicas contratantes dos serviços prestados pela Rodobens.

b) **Colaboradores:** são os administradores, corpo diretivo, funcionários, jovens aprendizes, estagiários, auxiliares ou quaisquer outros colaboradores da Rodobens.

c) **Dado(s) e/ou Informação (ões):** são todos os dados referentes às atividades desenvolvidas pela Rodobens na execução de seu objeto social, incluindo dados de Clientes, pessoais ou não, e classificados de acordo com o item III desta Política.

d) **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. São considerados incidentes, mas não se limitando a esses: (i) acesso indevido a contas e/ou sistemas da Rodobens; (ii) acessos não autorizado a bases de Dados ou Informações de uso interno ou confidencial da Rodobens; (iii) alteração ou perda de Dados ou Informações, ou de acesso a sistemas ou ambientes lógicos, bem como da integridade destes; (iv) vulnerabilidades existentes nos sistemas, bem como situações de indisponibilidade dos sistemas e/ou das informações ou (v) demais falhas de segurança que acarretem em acessos não autorizados a sistemas ou ambientes tecnológicos da Rodobens, por meio de técnicas, conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

e) **Prestador de Serviço:** pessoa física ou jurídica, devidamente contratada pela Rodobens, 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.

f) **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 Rodobens, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades da Rodobens.

g) **Serviços Relevantes:** Serviços prestados por Prestadores de Serviço à Rodobens cuja indisponibilidade, vulnerabilidade ou inconsistência possa prejudicar a continuidade de seus negócios: (i) afetando o atendimento ofertado ao Cliente; (ii) paralisando a operação da Rodobens, podendo causar perdas financeiras; ou (iii) impedindo o fornecimento de

informações pela Rodobens aos entes reguladores e/ou o cumprimento de direitos e garantias dos clientes.

2. BASES DA POLÍTICA

A presente Política foi elaborada considerando o porte, o perfil de risco e o modelo de negócio da Rodobens, 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 Rodobens.

3. OBJETIVO DA POLÍTICA

Esta Política tem por objetivo estabelecer e comunicar os princípios, valores, conceitos, procedimentos e controles que são adotados na prestação de serviços da Rodobens 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 Rodobens.

4. ABRANGÊNCIA

Os procedimentos abaixo descritos são direcionados a todos os Colaboradores e Prestadores de Serviços de todas as empresas do grupo Rodobens.

Em atenção ao disposto no artigo 2º, parágrafos 2º e 3º da Resolução nº 4.658/2018 do Banco Central do Brasil, foram adotados Política de Segurança Cibernética e Plano de Ação e de Resposta a Incidentes de Segurança da Informação únicos pelas Administradoras de Consórcio e Banco Rodobens S/A.

5. DOCUMENTOS REFERENCIADOS

i. Política de Segurança da Informação

ii. Política de Uso da Informação

iii. Política de Continuidade de Negócios

iv. Política de Gestão de Acessos a Redes e Sistemas

v. Política de Backup

vi. Política de Elegibilidade

vii. Plano de Ação e de Resposta a Incidentes

6. CLASSIFICAÇÃO DE DADOS

6.1 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 Rodobens:

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

ii. **Nível 02 - Somente Uso Interno** – Informação não aprovada para circulação fora da Rodobens como, por exemplo: memorandos internos, minutas ou atas de reuniões, procedimentos, rotinas operacionais e relatórios de projetos internos;

iii. **Nível 03 - 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 Rodobens, inclusive dados pessoais.

iv. **Informações Sensíveis**: Informações internas ou confidenciais críticas ao desenvolvimento das atividades da Rodobens, 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 Rodobens ao Cliente, a realização de operações da Rodobens e/ou o cumprimento de suas obrigações legais e/ou normativas.

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

7. PRÍNCIPIOS

7.1 A Rodobens 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 Rodobens 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.

8. DIRETRIZES GERAIS DE SEGURANÇA CIBERNÉTICA

8.1 A presente Política deverá ser cumprida e respeitada por todos os Colaboradores e Prestadores de Serviços da Rodobens. 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 Rodobens;

ii. Realizar a adequada classificação dos Dados, conforme os critérios e princípios indicados nos itens 6 e 7 desta 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: (i) da manutenção de softwares antivírus e firewall instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente atualizados em sua última versão; (iii) 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 Rodobens;

vii. Comunicar imediatamente o Comitê de Proteção de Dados, quaisquer descumprimentos à esta Política, bem como suspeita de intrusão no sistema, infraestrutura ou no acesso aos Dados, através do e-mail protecaodedados@rodobens.com.br.

viii. O **Comitê de Proteção de Dados** é uma equipe multidisciplinar, composta por profissionais de **Tecnologia da Informação, Jurídico, CRM, Controles Internos e Suprimentos**, capitaneado pelo **Superintendente de Tecnologia da Informação**. As atribuições do Comitê serão definidas em norma interna específica.

9. MEDIDAS DE SEGURANÇA, PROCEDIMENTOS E CONTROLES

9.1 Além das diretrizes gerais supramencionadas, a Rodobens 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 Rodobens, por meio de seu login, com inserção de sua senha pessoal e intransferível;

ii. Na hipótese de o Prestador de Serviços não possuir, em decorrência do Contrato, acesso ao ambiente da Rodobens, 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. 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;

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

viii. São realizados testes e varreduras para detecção de vulnerabilidades na infraestrutura da Rodobens, 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;

ix. A Rodobens 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;

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

xi. Deverão ser realizados treinamentos e avaliações, em periodicidade a ser definida pelo Comitê de Segurança da Informação e Proteção de Dados, 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;

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

9.2 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 Rodobens, bem como pelos prestadores de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Rodobens.

10. INCIDENTES DE SEGURANÇA

10.1 Os Incidentes de segurança serão classificados conforme sua relevância e de acordo com (i) a classificação dos Dados e Informações envolvidos; e (ii) o impacto na continuidade dos negócios da Rodobens, nas seguintes categorias:

Classificação dos Dados	Impacto no Negócio	Gravidade do Incidente	Prazo para Resposta	Prazo para Recuperação
Público	Baixo	Simples	A definir	A definir
Interno	Baixo	Simples	A definir	A definir
Interno	Médio	Moderado	A definir	A definir
Interno	Alto	Grave	A definir	A definir
Confidencial	Baixo	Grave	A definir	A definir
Confidencial	Médio	Gravíssimo	A definir	A definir
Confidencial	Alto	Gravíssimo	A definir	A definir
Sensível	Alto	Gravíssimo	A definir	A definir

10.1.1 São considerados, para a definição do impacto do incidente na continuidade do negócio da Rodobens:

a) **Baixo:** causa lentidão ou indisponibilidade no acesso a sistemas e/ou Dados, sem, entretanto, afetar o atendimento ao Cliente ou a realização de transações;

b) **Médio:** causa lentidão no atendimento ao Cliente, podendo, ainda, impedir o acesso a alguns serviços não essenciais; e

c) **Alto:** impede o atendimento ao Cliente e/ou a realização de transações.

10.1.2 Entendem-se por Resposta e Recuperação de Incidentes:

a) Resposta: tempo necessário para que sejam instauradas condições mínimas aceitáveis no período imediatamente após Incidentes; e

b) Recuperação: tempo para que sejam restabelecidas as condições operacionais originais.

10.1.3 Os prazos para Resposta e Recuperação serão contados em horas úteis, para incidentes Simples e Moderados, e em horas corridas, para incidentes Graves e Gravíssimos.

10.2 Os Planos de Resposta, de acordo com a gravidade apurada do Incidente, serão definidos pelo Comitê de Proteção de Dados, com base nas diretrizes constantes do Plano de Ação e de Resposta a Incidentes.

10.3 Incidentes deverão ser imediatamente comunicados ao Comitê de Proteção de Dados, para adoção das medidas descritas no Plano de Ação e de Resposta a Incidentes.

10.4 Em caso de Prestadores de Serviços, a ocorrência do Incidente deve ser imediatamente comunicada ao gestor do contrato na Rodobens, para que este realize a comunicação ao Comitê de Segurança da Informação.

10.5 Quando da ocorrência de Incidente, o Comitê de Proteção de Dados ficará responsável por coordenar a adoção das medidas visando a contenção e solução do Incidente, atribuindo responsabilidades às demais áreas envolvidas, englobando, entre outros aspectos, conforme delimitado no Plano de Ação e de Resposta a Incidentes: (i) a análise das causas do Incidente e de seus impactos; (ii) as medidas necessárias para estancar o Incidente e controlar seus efeitos; (iii) o plano de comunicação do Incidente aos Clientes e às autoridades, sem prejudicar as investigações do ocorrida e a identificação da causa raiz.

11. ESTRUTURA DE GERENCIAMENTO

11.1 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.

11.2 Mencionados acessos serão revistos periodicamente e cancelados tempestivamente ao término do contrato do Colaborador ou do Prestador de Serviço, podendo, ainda, serem revogados pelo Departamento de Tecnologia da Informação a pedido da área de Recursos Humanos ou do Comitê de Segurança da Informação.

11.3 O acesso a infraestrutura física na qual estão armazenados referidos dados seguirão as mesmas diretrizes constantes do item 9.1 acima.

11.4 A Rodobens 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 Rodobens: (i) são realizados periodicamente treinamentos e campanhas voltados aos Colaboradores e Prestadores de Serviços, incluindo avaliação de pessoal; e (ii) são fornecidas informações a Clientes e usuários sobre precauções na utilização de produtos e serviços financeiros da Rodobens.

11.5 A Rodobens manterá programas de capacitação e de avaliação periódica de pessoal referentes a esta Política.

11.6 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 Rodobens e deverá considerar, ao menos, os seguintes cenários para a realização de testes de continuidade de negócios:

a) 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 Rodobens;

b) Realização de testes de intrusão a base de dados contendo Informações Sensíveis da Rodobens;

c) Tempo de recuperação de acesso a informações de backup em caso de perda de Informações Sensíveis;

d) Estratégias para a recuperação de Informações Sensíveis e Serviços Relevantes.

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

13. COMPARTILHAMENTO DE INFORMAÇÕES SOBRE OS INCIDENTES RELEVANTES

A Rodobens 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, pela Rodobens, de serviços de processamento e armazenamento de dados e de computação em nuvem considerados relevantes nos termos dessa política, se dá de acordo com o disposto na Resolução 4.658/2018 do Conselho Monetário Nacional, conforme cláusulas inseridas em referidos contratos, devendo estes serem devidamente validados pelo Departamento Jurídico da Rodobens.

A decisão de contratação de Serviços Relevantes junto a Prestadores de Serviços externos deverá ser amparada nos seguintes critérios: **(i)** confirmação da capacidade técnica do Prestador de Serviço de cumprir o quanto disposto nesta Política e na legislação aplicável à segurança cibernética, por meio de auditoria ou da apresentação de declarações e/ou certificações pelo Prestador de Serviço; **(ii)** dificuldade ou impossibilidade técnica ou custo elevado para a execução do Serviço Relevante pela Rodobens em sua própria infraestrutura e **(iii)** a criticidade e relevância do serviços a ser contratado

A contratação de Serviços Relevantes junto a Prestadores de Serviços deverá ser validada pelo Comitê de Proteção de Dados em conjunto com a área solicitante da contratação, bem como comunicada previamente ao Banco Central do Brasil.

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, Rodobens solicitará autorização do Banco Central do Brasil para tal contratação, sendo que estas e suas obrigações ficarão condicionadas ao proferimento da solicitação.

Previamente à contratação de serviços relevantes de processamentos e armazenamento de dados e de computação em nuvem serão adotados os procedimentos previstos no artigo 12 da Resolução 4.658/18 que serão de responsabilidade do departamento Tecnologia da Informação.

15. GUARDA DE DOCUMENTOS

Pelo período de 05 (cinco) anos, a Rodobens armazenará e manterá a disposição do Banco Central do Brasil, os seguintes documentos:

a) Esta Política de Segurança Cibernética;
b) O Plano de Ação e de Resposta a Incidentes;
c) O relatório anual previsto no Plano de Ação e de Resposta a Incidentes;
d) Os documentos referentes à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, e os procedimento envolvidos nesta;
e) Documentos referentes à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem prestados no exterior;
f) Os contratos que tenham por objeto a prestação de serviços de processamento e armazenamento de dados e de computação em nuvem, sendo contados o prazo de 05 (cinco) anos de armazenamento, a contar de sua extinção; e
g) Os dados, registros e informações relativas aos mecanismos de acompanhamento e de controle da implementação e efetividade da Política de Segurança Cibernética, do Plano de Ação e de Resposta a Incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação dos citados mecanismos.

16. RESPONSABILIDADE

O corpo diretivo da Rodobens 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.

17. COMUNICAÇÃO

Em caso de dúvidas acerca desta Política, por favor, entre em contato com a Rodobens por meio do e-mail protecaodedados@rodobens.com.br.

18. PENALIDADES

As infrações a esta Política serão apuradas pelo **Comitê de Proteção de Dados,** podendo contar inclusive com o apoio do departamento **Auditoria Interna** e demais estruturas de controles das Empresas Rodobens e, uma vez comprovada a transgressão do colaborador, o mesmo poderá ser penalizado com advertência, suspensão do trabalho com prejuízo à remuneração e/ou demissão com justa causa.