Sumário

1. Objetivo

A presente Política de Segurança da Informação ("Política" ou "PSI") do Rede Brasil do Pacto Global (a "RBPG") estabelece princípios gerais de comportamento para funcionários e terceiros, juntamente com requisitos a serem seguidos para reduzir possíveis riscos e danos relacionados a ameaças internas ou externas, intencionais ou acidentais, que possam afetar a confidencialidade, integridade, disponibilidade, autenticidade e privacidade das informações. Isso garante a proteção e uso apropriado dos ativos e Recursos de Tecnologia da Informação e Comunicação (TIC) corporativos, visando assegurar a continuidade dos negócios e a conformidade com leis e regulamentos.

Além disso, a PSI formaliza o compromisso da RBPG em promover diretrizes estratégicas, responsabilidades e competências para garantir a proteção de seus ativos tangíveis e intangíveis.

2. Público-alvo

Este é um documento aplicável, a partir de sua publicação, aos Colaboradores da RBPG. A PSI possui valor jurídico e é aplicável imediatamente após sua publicação indistintamente.

3. Documentos Complementares

- Política de Governança de Proteção de Dados Pessoais da RBPG
- Plano de Resposta e Remediação a Incidentes de Privacidade da RBPG
- Plano de Resposta a Requisições de Titulares de Dados Pessoais da RBPG

4. Glossário

"Autoridade Nacional de Proteção de Dados" ou "ANPD" é a autoridade administrativa encarregada da Proteção de Dados Pessoais, um órgão da administração pública nacional responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais em todo o território brasileiro.

"Ameaça" é qualquer evento, ação ou entidade que representa um potencial perigo ou risco para a confidencialidade, integridade e disponibilidade das informações e dos sistemas.

"Análise de Riscos" é a identificação de ameaças potenciais, vulnerabilidades e impactos que podem afetar a confidencialidade, integridade e disponibilidade das informações.

"Ativo" é qualquer elemento físico ou lógico que esteja associado à manipulação, armazenamento, processamento ou transmissão de informações. Isso inclui não apenas dispositivos de hardware, como estações de trabalho, servidores, dispositivos de armazenamento e redes, mas também software, dados, documentos, pessoas e qualquer outro recurso que desempenhe um papel na gestão e proteção das informações da organização.

"Autenticidade" é garantia de que a origem, a identidade e a integridade das informações e dos usuários sejam genuínas e confiáveis.

"Colaboradores" são todos os empregados da RBPG, incluindo representantes legais, diretores, estagiários, aprendizes, terceirizados e qualquer outra pessoa que possua vínculo direto com a RBPG.

"Confidencialidade" é a garantia de que o acesso (visualização, modificação e compartilhamento) à uma informação seja obtida somente por pessoas autorizadas.

"Dados pessoais" são quaisquer dados relacionados a um indivíduo (pessoa natural) que é ou possa ser identificado a partir dos dados ou a partir dos dados em conjunto com outras informações

"Disponibilidade" é a garantia de que os sistemas de informação, recursos e dados estejam acessíveis e operacionais quando necessários.

"Encarregado" é a pessoa que na RBPG é a responsável por coordenar e por assegurar a conformidade com a Política de Governança e Proteção de Dados Pessoais, com a Legislação de Proteção de Dados e que atuará como canal da RBPG com os Titulares de Dados e com a Autoridade Nacional de Proteção de Dados.

"Gestão de Risco" é o processo sistemático de identificação, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação, visando proteger os ativos de informação e garantir a continuidade das operações.

"Incidente de Segurança da Informação" é quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento da confidencialidade, integridade ou disponibilidade da informação, colocando o negócio em risco.

"Integridade" é a garantia de que as informações e os dados permaneçam completos, precisos e inalterados ao longo do tempo, envolvendo a proteção contra modificações não autorizadas e manipulação indevida.

"Segurança da Informação" ou "SI" são as medidas adotadas para proteger a confidencialidade, integridade e disponibilidade das informações e dos sistemas.

"Software" é programa de computador.

"Titular(es) de Dados" é qualquer pessoa natural pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.

"**Tratamento ou Tratamento de Dados Pessoais"** é qualquer operação realizada com Dados Pessoais, como, por exemplo, a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

5. Papéis e Responsabilidades

Colaboradores	• Ler, compreender e cumprir integralmente os termos desta PSI, bem como as demais políticas e normativos da RBPG; • Encaminhar quaisquer dúvidas sobre a PSI e sua aplicação para a Equipe de Segurança da Informação; • Comunicar à Equipe de Segurança da Informação qualquer evento que viole esta Política; • Comunicar à Equipe de Segurança da Informação qualquer evento que coloque/possa vir a colocar

	em risco a segurança das informações ou dos recursos da RBPG, assim como danos, não conformidades ou riscos que tenham detectado; • Assinar o Contrato de trabalho que contém a cláusula 5. Obrigação de confidencialidade e receber o Aviso de Privacidade de Dados aos Colaboradores da RBPG, formalizando a ciência e o aceite integral das disposições da PSI, assumindo responsabilidade pelo seu cumprimento; • Responder pela inobservância da PSI e demais políticas e normativos da RBPG; • O acesso aos sistemas da RBPG é concedido de forma pessoal e intransferível. É vedado o compartilhamento das credenciais de acesso para fins que não estejam alinhados com as políticas e interesses da RBPG; • Os colaboradores são responsáveis pelos ativos da RBPG sob sua tutela e devem zelar por seu controle de acesso, evitando destruição, alterações ou a divulgação não autorizada; • Reportar e documentar, por meio dos canais adequados, qualquer incidente relacionado à segurança e privacidade da informação que seja identificado; • Participar dos treinamentos e ações de conscientização sobre Segurança da Informação; • É obrigatório seguir as diretrizes estabelecidas nesta PSI, assim como as demais políticas e normativos da RBPG O colaborador será responsabilizado por qualquer dano ou prejuízo causado à RBPG e/ou a

	terceiros, resultante da não conformidade com as diretrizes e normas mencionadas nesta PSI.
Gestores de Pessoas e/ou Processos	• Servir de modelo de conduta em relação à Segurança da Informação, mantendo uma postura exemplar e desmontando aos colaboradores a importância do cumprimento da PSI; • Demandar a assinatura do Contrato de trabalho que contém a cláusula 5. Obrigação de confidencialidade e receber o Aviso de Privacidade de Dados aos Colaboradores da RBPG, formalizando a ciência e o aceite integral das disposições da PSI, assumindo responsabilidade pelo seu cumprimento e Ciência da PSI pelos colaboradores, reforçando o cumprimento das regras e do sigilo e confidencialidade sobre as informações da RBPG, mesmo após o desligamento; • Solicitar assinatura de contrato com cláusula de confidencialidade antes da concessão de acesso à informações da RBPG, tanto de colaboradores quanto de prestadores de serviços; • Adaptar os procedimentos internos e demais normas sob sua responsabilidade para garantir conformidade com esta PSI.
Equipe de Tecnologia	• Configurar os equipamentos dos colaboradores, assim como sistemas e ferramentas utilizadas, cumprindo com os requisitos desta PSI; • Realizar testes periódicos para checar a eficácia dos controles utilizados e reportar à Diretoria os resultados e sugestões de alteração;

	• Mapear as melhores práticas do mercado e novas soluções de segurança, apresentando-as para a Diretoria, buscando a atualização e manutenção da qualidade em segurança da RBPG; • Alinhar com a Diretoria os procedimentos de resposta aos incidentes; • Buscar segurança especial para colaboradores em sistemas com acesso público; • Criar e manter registros de auditoria com um nível de detalhamento adequado para posterior rastreamento de fraudes e falhas; • Atribuir cada dispositivo e conta a um responsável identificável, garantindo que as informações de um usuário não sejam removidas definitivamente antes de disponibilizar o ativo para outro usuário; • Após solicitação formal, garantir o bloqueio de acesso de usuários por motivo de incidente, investigação, desligamento ou demais situações que exijam tais medidas; • Garantir a entrada de novos ativos apenas após verificação da existência de códigos maliciosos/indesejados, assim como proteger os ativos da RBPG contra esses códigos e demais vulnerabilidades, principalmente em processo de mudança; • Fixar as regras para instalação de hardware e software em ambiente de produção corporativo; • Controlar, preservar e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para a RBPG, assim como

	garantir a realização de auditorias de configurações técnicas e análise de riscos; • Planejar, implementar, fornecer e monitorar a capacidade de processamento, transmissão e armazenagem necessários para garantir a segurança das atividades da RBPG; • Comprometer-se com o uso, manuseio, guarda de certificados digitais e assinaturas.
Equipe de Segurança da Informação	• Propor os processos e metodologias visando a segurança da informação, como o sistema de classificação da informação e análise de risco; • Atuar na proposição e apoio de iniciativas que busquem a segurança dos ativos de informação da RBPG, assim como promover a conscientização dos colaboradores sobre a importância da segurança da informação para o negócio da RBPG; • Publicar e promover a PSI; • Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços; • Analisar criticamente incidentes de segurança; • Buscar alinhamento com as diretrizes corporativas da empresa.

6. Disposições Gerais

6.1. Proteção de Dados Pessoais

A RBPG respeita a privacidade e busca garantir a disponibilidade, integridade e confidencialidade dos Dados Pessoais, em todo o seu ciclo de vida, em qualquer formato de armazenamento ou suporte, tendo o mesmo nível de tratamento de informações confidenciais. A proteção de dados e a segurança da informação serão endereçadas a partir desta PSI e das demais políticas e normativos específicos para governança em privacidade, conforme previsto pela legislação e regulamentação pertinentes.

A RBPG aplicará as seguintes medidas de segurança da informação quanto à tratamento de Dados Pessoais:

- Tratamento autorizado nos termos da legislação de proteção de Dados Pessoais vigente;
- Registro das operações de tratamento de Dados Pessoais e atualização periódica do registro, realizando transferências de Agente de Tratamento de modo seguro e previsto contratualmente;
- Adoção de medidas de segurança para proteger os Dados Pessoais de acesso não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado ou ilícito;
- Eliminação segura dos Dados Pessoais ao término da finalidade, assim como a manutenção dos dados quando houver obrigação legal e/ou regulatória;
- Elaboração e manutenção de plano de resposta a incidentes.

Quando possível, a RBPG irá adotar:

- Processos de anonimização e pseudonimização;
- Protocolos de criptografia na transmissão e armazenamento;
- Elaboração de relatórios de impacto à proteção de Dados Pessoais.

O Encarregado é responsável por orquestrar as questões de Privacidade.

6.2. Propriedade das Informações e Sigilo

Os ativos tangíveis e intangíveis são de propriedade e responsabilidade da RBPG, assim como as informações armazenadas, geradas, manuseadas, acessadas, ou descartadas no exercício das atividades realizadas pelos colaboradores. Aos ativos deve ser garantido o uso exclusivamente para fins profissionais, sendo proibida a revelação de informação da RBPG sem a autorização da Diretoria, com exceção de informações públicas.

6.3. Propriedade Intelectual

A RBPG deve autorizar a utilização, em qualquer suporte, de suas obras intelectuais, softwares, desenhos industriais, marcas, identidade visual ou qualquer outro sinal distintivo, devendo o uso ser vinculado a atividades profissionais. Esta disposição se aplica a Internet e mídias sociais e a qualquer ativo de propriedade intelectual, atual ou futuro.

6.4. Classificação de Informação

Devem ser classificadas todas as informações de propriedade ou sob a responsabilidade da RBPG, com aplicação de controles específicos em todo o seu ciclo de vida. Com base nos princípios de disponibilidade, integridade e confidencialidade, deve ser seguida a seguinte classificação:

- **Públicas**: informações aprovadas para consulta irrestrita, com requisitos de proteção mais brandos, visto que sua divulgação não compromete a atividade da RBPG;

- **Internas**: dados, documentos ou conteúdos que são de propriedade e circulação restrita dentro da RBPG;

- **Confidenciais**: informações que possuem restrições de acesso e divulgação devido ao seu caráter sensível ou sigiloso, cuja divulgação seja passível de trazer prejuízos à pessoa ou a RBPG. As informações confidenciais são acessíveis apenas a pessoas autorizadas e designadas para lidar com esses dados;

- **Restritas**: informações sensíveis cujo acesso indiscriminado, mesmo de colaboradores da RBPG, pode gerar danos à empresa. São informações de teor estratégico da empresa e restritas ao corpo diretivo ou a áreas estratégicas.

As informações deverão ser devidamente rotuladas para facilitar a comunicação da classificação das informações e apoiar a automação da gestão e tratamento das informações. Os rótulos devem refletir o regime de classificação previsto nesta PSI e devem ser facilmente reconhecíveis.

6.5. Uso dos ativos

Os recursos tecnológicos ou informações disponibilizadas pela RBPG devem ser utilizados, de forma responsável, para o exercício de atividades profissionais, devendo ser solicitada a assinatura do Contrato de trabalho que contém a cláusula 5. Obrigação de confidencialidade e receber o Aviso de Privacidade de Dados aos Colaboradores da RBPG. É proibido o uso dos ativos da RBPG para declarações agressivas ou sexualmente ofensivas, difamação, visitas a sites ilegais que tratem de algum tipo de discriminação, entre outras ações não alinhadas com os valores da RBPG.

Cada usuário é responsável por suas credenciais de acesso, sendo seu dever a comunicação de qualquer suspeita de comprometimento dos sistemas.

6.6. Instalação de Software por usuários

O desenvolvimento interno e externo de softwares, bem como aquisições de mercado, deve garantir o cumprimento dos requisitos de segurança da informação e controles de acesso previstos nesta PSI, além de serem realizadas somente pela Equipe de TI. A Equipe de TI deverá, ainda, providenciar o que for necessário para regularizar a licença e o registro desses programas. O uso de softwares não autorizados e previamente homologados pela RBPG é vedado aos colaboradores.

6.7. Repositórios Digitais e Dispositivos Removíveis

O uso de repositórios digitais ou dispositivos removíveis não autorizados ou homologados é vedado aos colaboradores da RBPG. Para a transmissão ou armazenamento de informações de propriedade da empresa, devem ser utilizadas as ferramentas autorizadas pela Equipe de Tecnologia.

6.8. Aplicativos de Comunicação Instantânea

Somente poderão ser utilizados os aplicativos de comunicação instantânea autorizados e homologados pela RBPG para troca de informações corporativas.

6.9. Controle de Acesso

A RBPG gerencia o acesso, tanto digital quanto físico, aos seus ambientes, ativos e informações. Dessa forma, cada colaborador recebe uma identidade digital exclusiva, de uso pessoal e intransferível, e, quando aplicável, de conhecimento exclusivo.

Os sistemas utilizados pela RBPG deverão possuir recursos que possibilitem a administração dos acessos, através dos perfis dos colaboradores e alçadas definidas pela Diretoria.

As atividades ligadas à administração de acessos deverão ser contempladas por procedimentos formais, englobando desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

Cabe ao colaborador a responsabilidade pelo uso, proteção e confidencialidade de sua identidade digital, sendo estritamente proibido compartilhar, divulgar, armazenar, reproduzir, publicar ou utilizar suas credenciais, assim como as de terceiros, sem autorização.

6.10. Equipamentos pessoais (dispositivos *BYOD*)

A RBPG gerencia o acesso, tanto digital quanto físico, aos seus ambientes, ativos e informações. Dessa forma, cada colaborador recebe uma identidade digital exclusiva, de uso pessoal e intransferível, e, quando aplicável, de conhecimento exclusivo.

Os sistemas utilizados pela RBPG deverão possuir recursos que possibilitem a administração dos acessos, através dos perfis dos colaboradores e alçadas definidas pela Diretoria.

As atividades ligadas à administração de acessos deverão ser contempladas por procedimentos formais, englobando desde a criação de um usuário novo, passando pela administração de privilégios e senhas e incluindo a desativação de usuários.

Cabe ao colaborador a responsabilidade pelo uso, proteção e confidencialidade de sua identidade digital, sendo estritamente proibido compartilhar, divulgar, armazenar, reproduzir, publicar ou utilizar suas credenciais, assim como as de terceiros, sem autorização.

6.11. Gestão de Mudanças

Todas as mudanças, principalmente nos sistemas e na infraestrutura tecnológica da RBPG, deverão ser realizadas pela Equipe de TI, visando preservar os controles relacionados a disponibilidade, integridade, sigilo e autenticidade das informações.

6.12. Gestão de Incidentes

Os incidentes de Segurança da Informação serão tratados pelas Equipes de Tecnologia e de Segurança de Informação, e, conforme gravidade, escalados para grupo de trabalho a ser criado internamente. Incidentes específicos de privacidade envolvendo Dados Pessoais terão o envolvimento do Encarregado que, se necessário, comunicará o incidente à ANPD.

6.13. Gestão de Continuidade dos Negócios

Os processos, pessoas e tecnologia fundamentais para o desenvolvimento dos negócios da RBPG devem estar associados a um Plano de Continuidade dos Serviços de Tecnologia da Informação, incluindo medidas para restaurar as operações normais do ambiente de tecnologia dentro de um prazo adequado e acordado com as áreas de negócio.

O Plano de Continuidade dos Serviços da Equipe de Tecnologia deve prever a realização de testes periódicos e revisões para garantir o correto funcionamento das atividades de recuperação ou prevenção de incidentes, além disto, deve ser divulgado para conhecimento de todos os usuários do ambiente da RBPG.

6.14. Gestão de Riscos

A Gestão de Riscos é estruturada em processo sistemático de identificação, avaliação, tratamento e monitoramento dos riscos relacionados à segurança da informação, visando proteger os ativos de informação e garantir a continuidade das operações.

São englobados no processo de gestão de riscos os ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

6.15. Desenvolvimento de Aplicações

Os sistemas e aplicativos eventualmente desenvolvidos internamente pela RBPG ou adquiridos de terceiros devem estar de acordo com as melhores práticas de desenvolvimento seguro. Deve ser avaliado pela Equipe de Tecnologia o uso de componentes de código aberto, bem como os softwares necessários para a administração da RBPG ou seus programas. Monitoramento

A RBPG monitora seus ambientes físicos e virtuais, visando identificar alertas de incidentes ou identificação de eventos que comprometam a segurança da informação. Além disso, o monitoramento verifica a eficácia dos controles implementados internamente e a proteção de seu patrimônio e reputação.

Para o acesso a sistemas e recursos tecnológicos da RBPG, colaboradores e terceiros devem estar cientes que suas ações podem ser monitoradas e registradas, visando a segurança da informação.

Toda informação, seja ela administrada, armazenada ou gerada nos sistemas da RBPG, estão passíveis de monitoramento e auditoria, respeitando as legislações aplicáveis. A inspeção e auditoria poderá ser realizada sempre que considerado necessário pela RBPG, respeitando a privacidade, razoabilidade e proporcionalidade.

6.16. Processo de Contratação de Colaboradores

Contratações nas quais ocorra o compartilhamento de informações de propriedade ou sob a responsabilidade da RBPG ou a concessão de acesso aos seus ambientes ou ativos críticos, devem ser precedidos por termos de confidencialidade ou cláusulas contratuais relacionadas à segurança da informação.

Esta PSI deve ser divulgada a todos os novos colaboradores, mediante entrega e coleta de registro de ciência em fase de contratação pela área responsável.

6.17. Programa de Conscientização

Devem ser realizados regularmente programas de conscientização sobre a importância da prática de Segurança da Informação, reforçando as diretrizes da presente política e as responsabilidades dos colaboradores em seu cumprimento.

6.18. Auditorias

Devem ser realizadas auditorias regulares para verificação dos sistemas e redes, assim como sua integridade e níveis de segurança. Estas auditorias devem ser realizadas pela área interna ou por fornecedores reconhecidos e competentes.

Além das auditorias regulares, a RBPG pode auditar seus sistemas sempre que julgar necessário, respeitando a privacidade, razoabilidade e proporcionalidade.

6.19. Backup

É de responsabilidade do colaborador realizar o backup de seu próprio equipamento. O backup da rede e dos servidores serão realizados pela Equipe de Tecnologia, de acordo com os procedimentos definidos tendo como parâmetros a criticidade e risco dos ativos.

6.20. Segurança das transferências de informação

A transferência de arquivos do ambiente da RBPG para qualquer outra empresa, instituição ou órgão, somente poderá ser realizada pelos meios homologados pela Equipe de Segurança da Informação.

6.21. Mesa e Tela Limpa

Visando evitar e reduzir os riscos de exposição e vazamento de informações, é recomendado manter o local de trabalho organizado, assim como a área de trabalho do seu equipamento. As diretrizes da política de mesa e tela limpa se aplicam a todos os modelos de trabalhado, devendo ser observados os seguintes comportamentos:

- Notebooks e desktops, durante a ausência de seu usuário, devem ter seus acessos bloqueados e protegidos por senha;

- Fora do período de uso, documentos físicos deverão ser guardados em armários trancados;
- Informações sensíveis ou críticas para o negócio da organização devem ser trancadas em local separado e seguro (armário ou cofre);
- Não anotar informações sensíveis em quadros brancos;
- Evitar imprimir documentos apenas para leitura;
- Destruir documentos impressos antes de jogá-los fora e, sempre que possível utilizar máquinas desfragmentadoras;
- Informações sensíveis ou confidenciais, quando impressas em local coletivo, devem ser retiradas da impressora imediatamente;
- Recomenda-se não realizar qualquer tipo de cópia de tela (foto, screenshot etc.) que contenham dados confidenciais da RBPG, dados protegidos por sigilo ou Dados Pessoais;
- Não colocar ou comer refeições e lanches sobre a mesa para evitar que possíveis danos ocorram;
- Evitar colocar copos de água, suco, refrigerante ou café sobre a mesa para que possíveis danos não ocorram.

6.22. Comportamento em Reuniões

Participar de reuniões sobre temas sensíveis e/ou confidenciais em ambientes públicos requer uma abordagem cuidadosa para garantir a segurança da informação e a confidencialidade dos assuntos discutidos. Aqui estão algumas condutas e diretrizes que podem ser úteis:

- Se possível, escolha um local seguro e privado para realizar a reunião;
- Utilize salas de conferência com isolamento acústico e que ofereçam controle de acesso;

- Utilize fones de ouvido para manutenção da confidencialidade dos assuntos discutidos;
- Mantenha a pauta da reunião o mais restrita possível, abordando apenas os tópicos essenciais;
- Mantenha uma lista restrita de participantes autorizados;
- Certifique-se de que todos os participantes compreendam a natureza confidencial da reunião e concordem em manter a confidencialidade;
- Utilize meios seguros de comunicação, como linhas telefônicas criptografadas ou salas de videoconferência protegidas por senha;
- Evite discutir informações sensíveis por meio de canais públicos, como mensagens de texto não criptografadas ou redes sociais;
- Fale em volumes baixos e evite discutir detalhes sensíveis em locais públicos;
- Utilize códigos ou termos genéricos quando necessário, especialmente se houver a possibilidade de ser ouvido por terceiros;
- Limite a distribuição de documentos sensíveis, sejam eles físicos ou digitais, e marque-os como confidenciais;
- Recolha todas as cópias de documentos distribuídos após a reunião;
- Evite o uso de dispositivos eletrônicos pessoais durante a reunião.
- Desative as funções de gravação em dispositivos eletrônicos para evitar o registro não autorizado;
- Certifique-se de que todos os participantes estejam cientes das políticas e procedimentos relacionados à segurança da informação;

7. Responsabilidades

O uso indevido dos dispositivos pressupõe assumir todos os riscos da sua má utilização. Aqueles que utilizarem os dispositivos da RBPG de forma incorreta e fora do escopo original de uso, serão os únicos responsáveis por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venham causar à RBPG e/ou a outros terceiros.

8. Infrações e Violações

Qualquer violação das regras definidas nesta Política ou demais normativas da RBPG, ainda que por mera omissão ou tentativa, será formalmente analisada por grupo interno que será criado em referida ocasião. Independente da aplicação de medidas judiciais cabíveis, o grupo interno criado analisará o caso e aplicará as sanções cabíveis, , incluindo, mas não se limitando, no caso de colaborador, a advertência verbal ou escrita, a suspensão e a demissão ou, quanto ao fornecedor de serviços, a rescisão contratual e a aplicação de multas, preferencialmente calculadas sobre o proveito econômico eventual e indevidamente obtido ou, ainda, sobre o valor do dano causado à RBPG e/ou seus parceiros comerciais, direta ou indiretamente.

9. Revisão da Política

Esta Política deve ser revisada anualmente pela Equipe de Segurança da Informação, ou sempre que houver mudança relevante.

São Paulo, 31 de outubro de 2025.

Assinado por:
rachel maia
02B2F822FB7E431...
Rachel Maia
Presidente do Conselho de Administração

Signed by:
27A89E0F595A4B4...
Guilherme Xavier
Diretor Executivo

Assinado por:
Rodrigo Favetta
930FF0823CDB41B...
Rodrigo Favetta
Diretor de Engajamento e Parcerias