

Assunto **Política de Segurança Cibernética e da Informação**

Data 30 de maio de 2018

Páginas.

14

De Carlos Zanvettor e Rodrigo Gatti
Área Diretoria de Operações

Telefone

3509-6000

Para Clientes, administradores, gestores, funcionários e outros colaboradores das sociedades do Grupo Rio Bravo. Para efeitos do presente memorando, entende-se como Grupo Rio Bravo a Rio Bravo Investimentos S.A., a Rio Bravo Investimentos DTVM Ltda. e todas as empresas ligadas, coligadas ou controladas a/por esta(s).

Área

Este documento (“Política de Segurança Cibernética e da Informação”) tem como objetivo atender a resolução nº 4.658 do Banco Central do Brasil e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados pelos administradores, funcionários e / ou outros colaboradores das sociedades do Grupo Rio Bravo (“Colaboradores” e “Grupo Rio Bravo”, respectivamente) na sua atuação interna e com o mercado.

Este documento está dividido nas seguintes seções:

1. Atribuições;
2. Importância da Segurança da Informação;
3. Princípios da Segurança da Informação;
4. Regras do uso dos Recursos de Tecnologia
5. Regras para o Uso do Computador;
6. Regras para o Uso da Internet;
7. Regras para o Uso do Correio Eletrônico
8. Regras para o uso do Telefone
9. Linhas gerais de Comportamento Seguro
10. Gestão de Mudanças
11. Revisões de acesso
12. Dúvidas.
13. Controle de versões e aprovações

1. Atribuições

Este documento (“Política de Segurança da Informação”) tem como objetivo estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tangem as informações acessadas pelos administradores, funcionários e / ou outros colaboradores das sociedades do Grupo Rio Bravo (“Colaboradores” e “Grupo Rio Bravo”, respectivamente) na sua atuação interna e com o mercado.

O Grupo Rio Bravo incorpora em seus valores corporativos a convicção de que o exercício de suas atividades e a expansão de seus negócios devem se basear em princípios éticos, os quais devem ser compartilhados por todos os seus Colaboradores. Na constante busca do seu desenvolvimento e da satisfação dos clientes, o Grupo Rio Bravo busca transparência e cumprimento da legislação aplicável às atividades de administração e gestão de recursos de terceiros.

A publicação desta Política representa o compromisso de todos os que trabalham no Grupo Rio Bravo com os valores e as práticas fundamentadas na integridade, confiança e lealdade. Portanto, a constante busca do desenvolvimento do Grupo Rio Bravo e a defesa dos interesses dos clientes estarão sempre pautadas nas diretrizes aqui expostas.

A área de Riscos e Controles Internos é responsável pela implementação de um sistema de supervisão que demonstre que os controles de segurança da informação estão sendo devidamente executados e alinhados com os níveis adotados pela Rio Bravo.

A área de Riscos e Controles Internos está apta a detectar eventuais desvios de conduta que possam colocar em risco: Clientes/Investidores, colaboradores e Grupo Rio Bravo

2. Importância da Segurança da Informação

Os pilares da segurança da informação nos dão subsídios para proteger as informações da Rio Bravo. Portanto, quando mencionamos “segurança da informação” estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa. (ISO 27002 A.5.1.1)

O que é Política de Segurança da Informação?

Política de Segurança é um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável. (ISO 27002 A.5.1.1)

A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a empresa em locais públicos ou com pessoas estranhas ao nosso meio. (ISO 27002 A.5.1.1)

3. Princípios da Segurança da Informação

Os princípios básicos da segurança da informação são: confidencialidade, integridade e disponibilidade das informações. Outras características são: irrefutabilidade, autenticação e o controle de acesso. Os benefícios são evidentes ao reduzir os riscos com vazamentos, fraudes, erros, uso indevido, sabotagens, roubo de informações e diversos outros problemas que possam comprometer esses princípios básicos. (ISO 27002 A.5.1.1)

- **Confidencialidade:** Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntaria ou involuntariamente dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.
- **Integridade:** Garantia da veracidade da informação, pois a mesma não deve ser alterada enquanto está sendo transferida ou armazenada. Ameaça à segurança acontece quando uma determinada informação fica exposta ao manuseio por uma pessoa não autorizada, que efetua alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.
- **Disponibilidade:** Prevenção contra as interrupções das operações da empresa como um todo. Os métodos para garantir a disponibilidade incluem um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança. As ameaças à segurança acontecem quando a informação deixa de estar acessível para quem necessita dela.
- **Acesso controlado:** O acesso dos usuários à informação é restrito e controlado, significando que só as pessoas que devem ter acesso a uma determinada informação, tenham esse acesso. Ameaça à segurança acontece há descuido ou possível quebra da confidencialidade das senhas de acesso à rede.

4. Regras do Uso de Tecnologia

- Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na Rio Bravo ou para outras situações formalmente permitidas. (ISO A.6.1.3)
- Quando o usuário se comunicar através de recursos de tecnologia da Rio Bravo, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da empresa. (ISO A.7.1.3)
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia da Rio Bravo devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário. (ISO A.15.1.5)
- O uso dos recursos de tecnologia da Rio Bravo pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente. (ISO A.10.10.1)
- Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (softwares) instalados. (ISO A.6.1.3)
- Os recursos de tecnologia da Rio Bravo, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. (ISO A.6.1.3)
- Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Riscos e Controles Internos (ISO A.13.1.1)

5. Regras do Uso do Computador

a. Propriedade do computador

- O recurso computador disponibilizado para o usuário é de propriedade da Rio Bravo. (ISO A.7.1)

b. Disponibilização e uso

- O recurso computador disponibilizado para o usuário pela Rio Bravo tem por objetivo o desempenho das atividades profissionais desse usuário na organização.
- É necessário que o gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de infraestrutura, que autorizará tecnicamente e fará a liberação mediante a disponibilidade de recursos (ISO A.7.1)

- Todos os equipamento, softwares e permissões acessos devem ser testados, homologados e autorizados pela área de infraestrutura para uso na Rio Bravo. (ISO A.10.3)
- A Rio Bravo pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário. (ISO A.10.3)
- Cada computador tem o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da área de infraestrutura. (ISO A.7.1)
- A identificação do usuário ao computador é feita através do login e senha disponibilizado pela área de Infraestrutura, portanto ela é sua assinatura eletrônica.
- Será apenas permitido senha forte com 8 caracteres alfanuméricos, maiúsculos e minúsculos. A reutilização de senhas obedecerá ao ciclo mínimo de 5 vezes.
- É permitido apenas 3 tentativas máximas de autenticação de senha, sendo todas malsucedidas, será bloqueado o acesso.
- A senha possui validade de 180 dias e sua troca será solicitada automaticamente quando da expiração da mesma.

c. Programas utilizados no computador

- Os programas aplicativos, programas básicos (sistema operacional e ferramentas) e componentes físicos são implantados e configurados pela área de infraestrutura. (ISO A.7.1)
- É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da área de infraestrutura
- É desabilitado ao usuário implantar ou alterar componentes físicos no computador.

d. Verificação do computador e acessos

- A Rio Bravo mantém por 5 anos todos os logs de sistemas, e verifica regularmente, quaisquer desvios de padrão de todos os computadores, arquivos em rede, sejam softwares, hardwares ou acessos que não sejam autorizados pela área de infraestrutura e Compliance.

- Os acessos a equipamentos, softwares e respectivas permissões serão testados pela área de Infraestrutura de Tecnologia com validação da área de Riscos e Controles Internos a cada 6 meses.

e. Responsabilidades do usuário

- Cuidar adequadamente do equipamento. O usuário é o custodiante deste recurso.
- Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de infraestrutura.

g. Outras proteções

- É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente). (ISO A.11.5.5)
- É implantado o “log-off” automático por inatividade durante o período de 24 horas. (ISO A.11.5.5)
- É implantado o bloqueio do acesso as portas USB dos computadores para proteção contra vírus e cópia indevida dos dados contidos nos servidores. (ISO A.10.8)
- É implantado o bloqueio do acesso à sites de armazenamento de dados em nuvem (cloud) (ISO A.10.8)
- É implantado o bloqueio de sistemas de gerenciamento de computador a distância (ISO A.10.8)

h. Termo de compromisso

- Para ter acesso à informação da Rio Bravo, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pelo Comitê Gestor. (ISO A.8.1.3)
- O Compliance da Rio Bravo alerta todos os usuários que a instalação ou utilização de software não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, sujeitando os infratores à pena de detenção e multa. A Rio Bravo não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima.
- Todas as práticas que representam ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

6. Regras do uso da Internet

a. Responsabilidade e forma de uso

- O usuário é responsável por todo acesso realizado com a sua autenticação.

- O usuário é proibido de acessar endereços de internet (sites) que:
 - Possam violar direitos de autor, marcas, licenças de programas (softwares) ou patentes existentes.
 - Possuam conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia.
 - Conttenham informações que não colaborem para o alcance dos objetivos da Rio Bravo.
 - Defendam atividades ilegais. Menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes e que o uso do material foi autorizado pelo gestor da sua área.

c. Uso de serviço de mensagem instantânea.

- É proibido o uso de serviços de mensagem instantânea (MSN, etc), através dos computadores da Rio Bravo, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pelo Compliance.

d. Uso de serviço de rádio, TV, download de vídeos, filmes e músicas.

- É proibido o uso de serviços de rádio, TV, download de vídeos, filmes e músicas, através dos computadores da Rio Bravo, exceto em eventuais situações de uso profissional autorizado pelo gestor da área e pela área de infra-estrutura.

e. Bloqueio de endereços de Internet

- Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da Internet que não estejam alinhados com esta Política e com o Código de Ética da Empresa.

f. Uso de Correio Eletrônico particular tipo Webmail

- É proibido o acesso aos serviços de correio eletrônico particular, tipo Webmail, através dos recursos de tecnologia da Rio Bravo.

7. Regras do Uso do Correio Eletrônico (E-mail)

a. Endereço eletrônico do usuário

- A Rio Bravo disponibiliza endereços de seu correio eletrônico para utilização do usuário no desempenho de suas funções profissionais. (ex.: usuario@riobravo.com.br)
- O endereço eletrônico disponibilizado para o usuário é individual, intransferível e pertence à empresa.
- O endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a Rio Bravo.
- Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela área de infra-estrutura e registrada para possibilitar uma posterior verificação de autoria.

b. Criação, manutenção e exclusão do endereço de correio eletrônico

- A utilização desse endereço de correio eletrônico pelo usuário necessita ser autorizada pelo seu Gestor.
- A liberação do endereço de correio eletrônico será feita pela área de infraestrutura de maneira controlada e segura com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço.
- Quando acontecer desligamento de usuário, o Gestor deve comunicar à área de infraestrutura o nome e a identificação desse usuário.
- As caixas postais de contas de correio eletrônico da Rio Bravo tem limite de tamanho de 3.2GB e as mensagens enviadas/recebidas poderão conter arquivos anexos com até 8MB por mensagem.

c. Endereço eletrônico de programas ou de comunicação corporativa

- É permitido que um programa aplicativo ou um programa de sistema possua um endereço de correio eletrônico. Nesse caso, é obrigatória a existência de um usuário da área de infraestrutura responsável por acompanhar as mensagens emitidas e recebidas por esse endereço.
- É permitido a existência de endereços de correio eletrônico para o envio de mensagens tipo Comunicação Interna da Rio Bravo, porém, é obrigatória a identificação do usuário que encaminhou a mensagem.

d. Acesso à distância

- O usuário pode acessar o seu endereço eletrônico cedido pela Rio Bravo mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via Internet (Web Mail).
- O acesso ao endereço da Rio Bravo na Internet deve ser autenticado via certificado digital.

e. Propriedades do endereço

- O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da Rio Bravo.
- Em situações autorizadas pela Diretoria, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela Rio Bravo ou por pessoas/entidades por ela indicada. Não deve ser mantida portando, expectativa de privacidade pessoal.

f. Responsabilidades e forma de uso

O usuário que utiliza um endereço de correio eletrônico:

- É responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu e-mail.
- Pode enviar mensagens necessárias para o seu desempenho profissional na Empresa.
- É proibido criar, copiar ou encaminhar mensagens ou imagens que:
 - Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
 - Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais.
 - Repassem propagandas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Empresa, a sugestão deve ser encaminhada para a Área de Recursos Humanos, que definirá a sua publicação ou não.
 - Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física.
 - Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.
 - Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros.
 - Defendam ou possibilitem a realização de atividades ilegais.
 - Sejam ou sugiram a formação ou divulgação de correntes de mensagens.
 - Possam prejudicar a imagem da Rio Bravo.
 - Sejam incoerentes com o nosso Código de Ética.

- É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.
- Deve estar ciente que uma mensagem de correio eletrônico da Rio Bravo é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade.
- Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da Rio Bravo.
- Deve observar se o endereço do destinatário corresponde realmente ao destinatário desejado.
- Deve ser diligente em relação:
 - Aos usuários que receberão a mensagem (Destinatário/ To, Copiado/Cc e Copiado Oculto/Bcc);
 - Ao nível de sigilo da informação contida na mensagem;
 - Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
 - Ao uso da opção Encaminhar (Forward), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.
- Deve deixar mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto para quem deve ser enviada a mensagem.

g. Cópias de segurança

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria (ISO A.10.5.1):

- A cópia de segurança das mensagens de correio eletrônico é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infra-estrutura.
- A área de infra-estrutura fornecerá o serviço de recuperação de mensagens de correio eletrônico, a partir de arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecido.

8. Regras do Uso de Telefone

a. Número do telefone do usuário

- A Rio Bravo disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais.
- Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela área de infra-estrutura e registrada para possibilitar uma posterior verificação de autoria.

b. Propriedades do número do telefone

- O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade da Rio Bravo.
- Todos os telefones são gravados e monitorados regularmente, e em situações especiais autorizadas pelo Comitê Gestor, as conversas de um usuário poderão ser acessadas pela Rio Bravo ou por pessoas/entidades por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal.

c. Responsabilidades e forma de uso

O usuário que utiliza um telefone:

- É responsável por todo conteúdo da conversa.
- Pode utilizar o telefone para o seu desempenho profissional na empresa.
- É proibido utilizar o telefone para conversas que:
 - Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza.
 - Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física.
 - Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional.
 - Defendam ou possibilitem a realização de atividades ilegais.
 - Possam prejudicar a imagem da Rio Bravo.
 - Sejam incoerentes com o nosso Código de Ética.

d. Cópias de segurança

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:

- A cópia de segurança dos telefonemas é feita de forma centralizada no ambiente dos equipamentos servidores corporativos, sob a responsabilidade da área de infraestrutura.
- A área de infra-estrutura apenas fornecerá a recuperação de telefonemas, a partir de arquivos de cópia de segurança, em situações autorizadas pelo Comitê Gestor.

9. Linhas Gerais de Comportamento

Controle de acesso e câmeras de gravação

O controle de acesso é parte central da segurança de uma empresa do ponto de vista da segurança da informação. Por isso, é fundamental que ao entrar nas dependências da Rio Bravo seja incluída seu crachá, mesmo que a porta já esteja aberta.

Câmeras de gravação de vídeo foram instaladas nas dependências da Rio Bravo para garantir a sua segurança.

No ambiente externo, é melhor ficar atento

Falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma empresa.

Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa da empresa. Qualquer pendrive ou conexão de rede pode conter dados valiosos.

Cuidado com o lixo que você produz

O lixo pode ser uma fonte de informações para pessoas mal-intencionadas.

Destrua os documentos que contenham informações sensíveis, pessoais ou da Rio Bravo antes de descartá-los. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, rasgue-o antes de jogá-lo fora.

Cuidados com senhas e acessos no sistema

Cada tarefa desenvolvida na Rio Bravo precisa ter um responsável.

A única forma de saber o responsável por cada atividade é através da identificação do usuário. Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso. Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

Alguns exemplos de ações que podem ser atribuídas a você, são:

- Liberação de ações indevidas;
- E-mails com informações inadequadas;

- Acesso a páginas da internet proibidas;

Compartilhar sua senha é como assinar um cheque em branco. É permitido apenas a utilização senhas fortes, isto é, com mais de 8 caracteres, combinando numéricos e alfanuméricos, maiúsculas e minúsculas e não utilize datas comemorativas, sobrenomes, nome do cônjuge, nome dos filhos, placas de carro, etc. Não escreva a senha em local público ou de fácil acesso

Adote um comportamento seguro

- Não compartilhe nem divulgue sua senha a terceiros;
- Não transporte informações confidenciais da Rio Bravo em qualquer meio (CD, DVD, pendrive, papel, etc.) sem as devidas autorizações e proteções;
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais, etc.);
- Não abra mensagens de origem desconhecida
- Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contêm informações confidenciais;
- Siga corretamente a política para uso de internet e correio eletrônico estabelecida pela Rio Bravo.

10. Gestão de mudanças (GMUD)

A área de Infraestrutura de IT é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de acesso, hardware e software ou que tenha impacto direto na infraestrutura de negócio ou operacional do grupo Rio Bravo.

As solicitações devem ser encaminhadas do gestor responsável pela solicitação para área de infraestrutura de IT, e tais demandas devem ser registradas em sistema para acompanhamento histórico.

11. Revisões de acessos

A área de Riscos/Controles Internos e Infraestrutura de IT são responsáveis por liderar anualmente os processos de revisões de acessos físicos ou lógicos de todos os colaboradores do Grupo Rio Bravo e propor a alteração e sua respectiva implementação.

12. Duvidas

Quaisquer dúvidas relacionadas com a presente política devem ser esclarecidas com a Diretoria de Operações do Grupo Rio Bravo ou com a área de Risco e Controles Internos.

13. Controle de versões e aprovações

Código referência da política	Área Emissão	Número Páginas	Data aprovação	Nome Responsável	Nome Aprovador
PGC_07	Compliance	14	17-10-15	Rodrigo Gatti	Eros Dalhe
PGC_07	Compliance	14	01-03-16	Rodrigo Gatti	Eros Dalhe
PGC_07	Compliance	14	02-03-17	Rodrigo Gatti	Eros Dalhe
PGC_07	Compliance	14		Rodrigo Gatti	

PGC = Políticas relacionadas aos Controles Corporativos