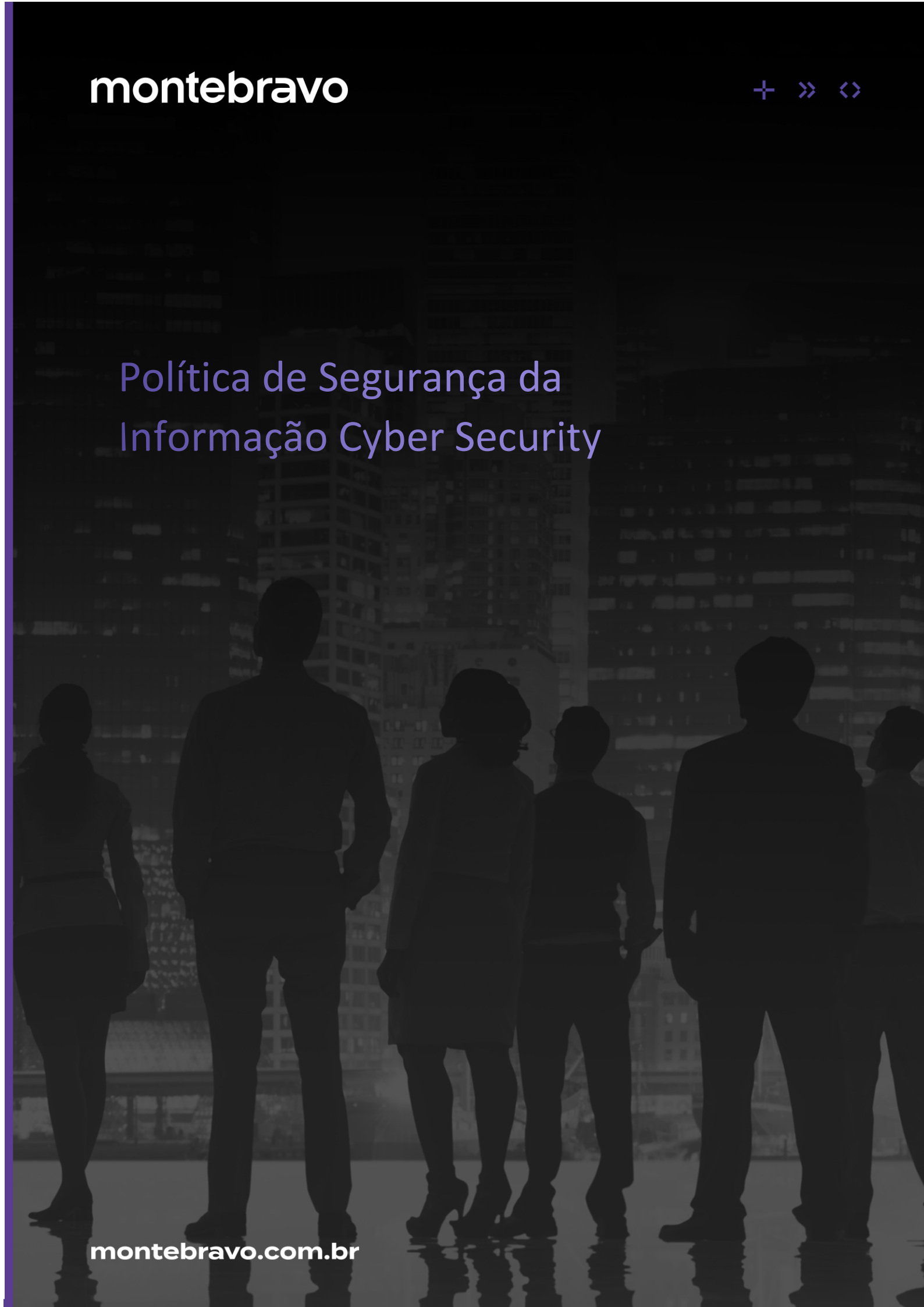
montebravo

Política de Segurança da Informação Cyber Security



montebravo.com.br

Controle do Documento			
Código:	POL_PSI_01	**Periodicidade:**	Anual
Criação	01 de junho de 2023	**Gestão:**	Compliance
Revisão:	-	**Versão:**	V 1.0
Elaborador:	Gilmar Maciel	**Aprovador(es):**	CGSI
Revisor:	Marcelo Halmel	**Classificação:**	USO EXTERNO

Sumário

1. Objetivo 4
2. Vigência 5
3. Abrangência 5
4. Princípios da Segurança da Informação 5
5. Estrutura Normativa de Segurança da Informação e Continuidade de Negócio 6
6. Diretrizes Gerais 6
6.1. Proteção da Informação 7
6.2. Privacidade da Informação 8
6.3. Classificação da Informação 8
6.4. Classificação da Informação 9
6.5. BACKUP 10
6.6. CPD 10
6.7. SENHAS 11
6.8. Monitoramento e Auditoria do Ambiente 11
6.9. Uso e Acesso à Internet 12
6.10. Gestão de Riscos 12
6.11. Vulnerabilidades 12
6.12. Gestão de Continuidade 13
6.13. Programa de Cyber Security 14
6.14. Programa de Conscientização de Cyber Segurança 14
6.15. Tratamento de Incidentes de Segurança da Informação 14
6.16. Atribuições e Responsabilidades 15
6.16.1. Integrantes 15

6.16.2. Comitê Gestor de Segurança da Informação 16
6.16.3. Diretoria (Alta Direção) 16
6.16.4. Líder da área ou departamento 17
6.16.5. Proprietário da Informação 17
6.16.6. Jurídico 17
6.16.7. Departamento Pessoal, Recursos Humanos, Treinamento e Desenvolvimento 18
6.16.8. Segurança da Informação 18
7. Regulamentação e Legislação Aplicáveis 19
8. Penalidades e Sanções 20
9. Disposições Finais 20

1. Objetivo

A presente Política de Segurança da Informação e Cyber Security ("política") constitui uma declaração formal da MONTE BRAVO CORRETORA DE TÍTULOS E VALORES MOBILIÁRIOS S.A. ("Monte Bravo"), acerca de seu compromisso com a proteção das informações de sua propriedade, devendo ser observado por todos os seus sócios e integrantes. Seu propósito é formalizar o direcionamento estratégico acerca da gestão de segurança da informação, estabelecendo as diretrizes a serem seguidas para implantação, operação, manutenção, controle e melhoria contínua do seu SGSI, guiando-se, principalmente, pelos conceitos e orientações das normas ABNT ISO/IEC da família 27000.

Esta política resume os princípios da Segurança da Informação que a Monte Bravo reconhece como sendo importantes, devendo estar presentes no cotidiano de suas atividades. Assim, visa assegurar a confidencialidade, disponibilidade e integridade do processamento, transferência, manuseio e armazenamento das informações críticas que estão no escopo do Sistema de Gestão de Segurança da Informação (SGSI). Os objetivos definidos desta política são:

- Manter avaliações de riscos de segurança da informação dentro do escopo do SGSI conforme a norma de risco da Monte Bravo;
- Manter os níveis aceitáveis de risco residual para a organização;
- Garantir níveis aceitáveis de confidencialidade, integridade e disponibilidade das informações críticas;
- Atender aos requisitos regulamentares e legislativos;
- Apoiar a produção, manutenção e teste dos planos de continuidade de negócio assim como a sua praticabilidade contida na Política de Gestão de Continuidade de Negócio;
- Realizar o treinamento e a conscientização da segurança da informação para todos os integrantes da Monte Bravo;
- Relatar a avaliação de todas as violações da segurança da informação e vulnerabilidades para as partes interessadas.

A Política de Segurança da Informação também demonstra o comprometimento da Monte Bravo com a Segurança da Informação, com o apoio de todos os integrantes, e todos aqueles que estão diretamente envolvidos na sua aplicação. Todos os integrantes que tenham qualquer envolvimento com os ativos e informações críticas coberto pelo escopo do SGSI são responsáveis por seguir a política, as diretrizes, as normas e os procedimentos de segurança da informação da Monte Bravo. Este documento foi

aprovado formalmente pelo CGSI - Comitê Gestor de Segurança da Informação da Monte Bravo.

2. Vigência

Esta política entra em vigor a partir da sua publicação e deve ser revisada com periodicidade mínima de 1 ano, ou quando da ocorrência de eventos considerados relevantes pela Monte Bravo, ou conforme definido nos termos da regulamentação aplicável.

3. Abrangência

As diretrizes e procedimentos estabelecidos no desenvolvimento da presente política serão aplicáveis a todos os integrantes, terceiros, parceiros e prestadores de serviços relevantes, relacionados diretamente com as atividades da empresa.

4. Princípios da Segurança da Informação

Os princípios da segurança da informação abrangem, basicamente, os seguintes aspectos:

- Integridade: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;
- Confidencialidade: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;
- Disponibilidade: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Toda informação deve ser protegida conforme as regras definidas nesta política. A adoção de procedimentos que garantam a segurança da informação deve ser prioridade constante nas áreas da Monte Bravo, de forma que se possa reduzir falhas e danos que possam comprometer a imagem da empresa ou trazer prejuízos a outrem.

Toda informação produzida ou recebida pelos integrantes como resultado da atividade profissional contratada pela Monte Bravo pertence à referida instituição, ou seja, Monte Bravo. As exceções devem ser explícitas e formalizadas em contrato entre as partes. Isto também se aplica para os equipamentos de informática, comunicação, sistemas e informações utilizados pelos integrantes para a realização das atividades profissionais. O uso pessoal dos recursos e equipamentos é permitido desde que esteja devidamente autorizado e não prejudique o desempenho dos sistemas e serviços da Monte Bravo.

A Monte Bravo, por meio da Segurança da Informação e outras áreas ligadas ao tema, poderá registrar e monitorar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas. Os critérios e requisitos

estabelecidos nesta PSI deverão ser aplicadas em todas as áreas da Monte Bravo, suas dependências e outras unidades que possam a vir a ser constituídas.

5. Estrutura Normativa de Segurança da Informação e Continuidade de Negócio

A estrutura normativa de Segurança da Informação e Continuidade de Negócio da Monte Bravo é composta por três níveis hierárquicos de documentos, relacionados a seguir:

Nível Hierárquico de documentos de Segurança da Informação e Continuidade de Negócio		
Documento	Descrição	Aprovação e Revisão
Política (Nível estratégico)	Constituída do presente documento, aplica a estrutura, estabelece as diretrizes e define as responsabilidades referentes à segurança da informação que representam os princípios básicos que a Monte Bravo decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção. Serve como base para que as normas e os procedimentos sejam criados e detalhados	Aprovação: Comitê Gestor de Segurança da Informação - CGSI Revisão: anual ou quando ocorrer mudanças no SGSI.
Normas (Nível Tático)	Estabelecem regras básicas de como deve ser implementado o controle que foi definido pela Política ou algum regulamento que a organização deve seguir para ficar em conformidade.	Aprovação: Segurança da Informação Revisão: anual ou quando ocorrer mudanças significativas no SGSI.
Procedimentos (Nível Operacional)	Contêm atividades que detalham como o controle deve ser implementado, assim como sua manutenção e operação	Aprovação: Gestores das áreas e/ou Gestor de Segurança da Informação Revisão: anual ou quando ocorrer mudança significativa no procedimento.

6. Diretrizes Gerais

Orientações específicas e procedimentos próprios deverão ser fixados em normas e procedimentos complementares, considerando os tópicos abaixo das diretrizes gerais de segurança da informação da Monte Bravo.

6.1. Proteção da Informação

Define-se como necessária a proteção da informação da empresa, especialmente, de sua propriedade e informação imprescindível como fator primordial nas atividades profissionais de cada integrante da Monte Bravo, sendo que:

- Os integrantes devem assumir uma postura proativa no que diz respeito à proteção das informações da Monte Bravo e devem estar atentos a ameaças externas, bem como fraudes, roubo de informações, e acesso indevido aos sistemas de informação sob responsabilidade da Monte Bravo;
- As informações não podem ser transportadas em qualquer meio físico, sem as devidas proteções e autorizações;
- Assuntos sigilosos classificados com confidenciais não devem ser expostos publicamente;
- Senhas, chaves e outros recursos de caráter pessoal são considerados intransferíveis e não podem ser compartilhados e divulgados;
- Somente softwares homologados podem ser utilizados no ambiente computacional da Monte Bravo;
- Documentos impressos e arquivos contendo informações confidenciais devem ser armazenados e protegidos. O descarte deve ser feito na forma da legislação pertinente;
- Todo usuário, para poder acessar dados das redes de computadores utilizadas pela Monte Bravo, deverá possuir um login ou usuário de acesso atrelado à uma senha previamente cadastrada, sendo este pessoal e intransferível, ficando vedada a utilização de login ou usuário de acesso genérico ou comunitário, exceto previamente autorizada;
- Os dados que necessitam de compartilhamento devem ser alocados nos servidores apropriados, atentando às permissões de acesso aplicáveis aos referidos dados;
- Todos os dados considerados como imprescindíveis aos objetivos da Monte Bravo devem ser protegidos através de rotinas sistemáticas e documentadas de cópia de segurança, devendo ser submetidos aos testes periódicos de recuperação;
- O acesso às dependências da Monte Bravo deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade, garantindo a rastreabilidade e a efetividade do acesso autorizado;
- O acesso lógico aos sistemas computacionais disponibilizados pela Monte Bravo deve ser controlado de maneira que sejam aplicados os princípios da integridade, confidencialidade e disponibilidade da informação, garantindo a rastreabilidade e a efetividade do acesso autorizado;
- São de propriedade da Monte Bravo todas as criações, códigos ou procedimentos desenvolvidos por qualquer colaborador durante o curso de seu vínculo com a empresa, nos limites legais (Leis nº 9.279/96, 9.609/98 e as demais aplicáveis);

- Documentos imprescindíveis para as atividades da empresa deverão ser salvos em local apropriado (rede ou diretório em nuvem do colaborador). Tais arquivos, se gravados apenas localmente nos computadores, não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no mesmo, sendo, portanto, de responsabilidade do próprio colaborador;
- Arquivos pessoais e/ou não pertinentes às atividades diretas da Monte Bravo não deverão ser copiados ou movidos para os diretórios da companhia, pois podem sobrecarregar o armazenamento nos servidores. Caso identificados, os arquivos poderão ser excluídos definitivamente sem necessidade de comunicação prévia ao colaborador;
- Os projetos gerenciados e realizados pela Monte Bravo deverão adotar critérios de segurança da informação para o cumprimento desta política.

6.2. Privacidade da Informação

Define-se como necessária a privacidade das informações que são manipuladas ou armazenadas nos meios às quais a Monte Bravo detém total controle administrativo, físico, lógico e legal. As diretivas abaixo refletem os valores institucionais da Monte Bravo e reafirmam o seu compromisso com a melhoria contínua desse processo:

- As informações são geradas, manipuladas, recebidas, tratadas e armazenadas de forma segura e íntegra, com métodos apropriados de segurança, podendo utilizar criptografia ou certificação digital, quando aplicável;
- As informações são acessadas somente por pessoas autorizadas e capacitadas para seu uso adequado;
- As informações podem ser disponibilizadas a quem tem direito de acesso, sendo exigido o cumprimento de nossa política e diretivas de segurança e privacidade de dados;
- As informações somente são fornecidas a terceiros, mediante autorização prévia da Monte Bravo, ou do cliente, ou para o atendimento de exigência legal ou regulamentar;
- As informações e dados constantes de nossos cadastros, bem como outras solicitações que venham garantir direitos legais ou contratuais só são fornecidos aos próprios interessados, mediante solicitação formal, seguindo os requisitos legais vigentes.

6.3. Classificação da Informação

Define-se como necessária a classificação da informação de propriedade da Monte Bravo, de maneira proporcional ao seu valor para a empresa, para possibilitar o controle adequado da mesma, devendo ser utilizados os seguintes níveis de classificação:

Classificação da Informação		
Tipo de Classificação	Descrição da Classificação	Aprovação da Informação
Confidencial	É a informação crítica para os negócios da Monte Bravo. A divulgação não autorizada dessa informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e criminais à Monte Bravo. É sempre restrita a um grupo específico de pessoas devidamente autorizadas. Deve ser acessada com restrições por colaboradores e prestadores de serviços da Monte Bravo, sob um contrato vigente e assinatura do NDA.	Aprovação: Líderes.
Interna	É uma informação da Monte Bravo que ela não tem interesse em divulgar, mas cujo acesso por parte de indivíduos externos à empresa pode ser evitado. Caso esta informação seja acessada indevidamente, poderá causar danos à imagem da Organização, porém, não com a mesma magnitude de uma informação confidencial. Pode ser acessada sem restrições por todos os colaboradores e prestadores de serviços da MB PARTICIPAÇÕES, sob um contrato vigente e assinatura do NDA.	Aprovação: Líderes.
Pública	É uma informação da Monte Bravo com linguagem e formato dedicado à divulgação ao público em geral, sendo seu caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação vigente que exija publicidade da mesma.	Aprovação: Colaboradores.

6.4. Classificação da Informação

Define-se como necessário controle de acesso da Monte Bravo, as seguintes diretrizes abaixo:

- O controle de acesso deverá considerar e respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação da Monte Bravo.
- A criação e administração de contas será realizada de acordo com procedimento específico para todo e qualquer usuário. Para o usuário que não exerce funções de

administração de rede, sistema ou qualquer atividade de gerenciamento, suporte e operação, será privilegiada a criação de uma única conta institucional de acesso, pessoal e intransferível. Contas com perfil de administrador somente serão criadas para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

- As práticas de segurança deverão contemplar procedimentos de acesso físico a áreas e instalações, gestão de acessos e delimitação de perímetros de segurança dos datacenters;
- O uso do correio eletrônico da Monte Bravo é para fins corporativos e relacionados às atividades primariamente da empresa.

6.5. BACKUP

Define-se como necessário controle de acesso da Monte Bravo, as seguintes diretrizes abaixo:

- O serviço de backup deve ser aplicado por sistemas informacionais próprios considerando, inclusive, a execução agendada fora do horário de expediente normal da empresa, se possível, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de colaboradores ou processos automatizados aos sistemas de informática;
- A solução de backup deverá ser mantida atualizada, considerando suas diversas características (atualizações de correção, novas versões, ciclo de vida, garantia, melhorias, entre outros);
- A administração das mídias de backup, quando aplicável, deverá ser contemplada nas normas complementares sobre o serviço, objetivando manter sua segurança e integridade;
- As mídias de backups históricos ou especiais deverão ser armazenadas em instalações seguras, preferencialmente com estrutura de cofres e salas-cofres;
- Os backups críticos para o bom funcionamento dos serviços da Monte Bravo exigem uma regra de retenção especial, a ser prevista nos procedimentos específicos e de acordo com as normas estabelecidas, seguindo ainda as determinações fiscais e legais existentes no país;
- A execução de rotinas de backup e restore deverá ser controlada nos termos das normas e procedimentos próprios.

6.6. CPD

Define-se como necessário as seguintes diretrizes da Monte Bravo:

- O acesso físico ao CPD deverá ser feito por sistema forte de autenticação. O acesso físico por meio de recursos mecânicos-manuais apenas poderá ocorrer em situações de emergência, quando a segurança física do data center estiver comprometida,

como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação forte não estiver funcionando.

- O acesso ao CPD por visitantes ou terceiros somente poderá ser realizado com autorização de um integrante da Monte Bravo, que deverá preencher a solicitação de acesso prevista, conforme estabelecida na norma própria.
- A lista de funções com direito de acesso ao CPD deverá ser constantemente atualizada, de acordo com os termos de norma própria, salva em locais seguros e apropriados.

No caso de desligamento de usuários que possuam acesso ao CPD, imediatamente deverá ser providenciada a sua exclusão do sistema de autenticação forte e da lista de usuários autorizados.

6.7. SENHAS

Define-se como necessário da MB PARTICIPAÇÕES, as seguintes diretrizes abaixo:

- A senha é pessoal e intransferível, não deve ser compartilhada;
- Todas as senhas dos sistemas da MB Participações devem possuir tamanho mínimo de 8 caracteres;
- A senha deve conter pelo menos: um caractere maiúsculo, um caractere minúsculo, um número e um símbolo;
- É recomendável o bloqueio do usuário após a quinta tentativa de login incorreto. O desbloqueio deve ser de forma automática, após 20 minutos ou pelo administrador do sistema;
- A senha padrão deve ser trocada no primeiro acesso;
- Recomenda-se habilitar o histórico das últimas seis senhas, não permitindo a repetição da mesma;

A senha deve ser armazenada de forma criptografada.

6.8. Monitoramento e Auditoria do Ambiente

Define-se como necessário as seguintes diretrizes da Monte Bravo:

- Permitir o monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede, de modo que a informação gerada por esses sistemas possa ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- Tornar disponível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Departamento Jurídico;
- Realizar, a qualquer tempo, inspeção física e/ou lógica nos equipamentos e informações de propriedade da Monte Bravo;

- Permitir mecanismos e práticas de proteção preventivos, detectáveis, ou corretivos para garantir segurança das informações e dos perímetros de acesso físico;
- Desinstalar, a qualquer tempo, qualquer software ou sistema que represente risco ou esteja em não conformidade com as políticas, normas e procedimentos vigentes.

6.9. Uso e Acesso à Internet

Define-se como necessário as seguintes diretrizes da Monte Bravo:

- Qualquer informação que seja acessada, transmitida, recebida ou produzida na internet está sujeita à monitoria e auditoria. Portanto, a Monte Bravo, em total conformidade legal, reserva-se o direito de monitorar e registrar os acessos à rede mundial de computadores;
- Os equipamentos, tecnologias e serviços fornecidos para o acesso à internet são de propriedade da Monte Bravo, que pode analisar e, se necessário, bloquear qualquer arquivo, site, caixa postal de correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando a assegurar o cumprimento de sua Política de Segurança da Informação.

6.10. Gestão de Riscos

As diretrizes gerais do processo de Gestão de Riscos de Segurança da Informação da Monte Bravo deverão considerar, prioritariamente, os objetivos estratégicos, os processos críticos, os requisitos legais e a estrutura da empresa, além de estarem alinhadas a esta Política de Segurança da Informação. Esse processo deverá ser contínuo e aplicado na implementação, operação, manutenção, controle e melhoria contínua do Sistema de Gestão de Segurança da Informação e do Sistema de Gestão de Continuidade de Negócio.

6.11. Vulnerabilidades

A MB PARTICIPAÇÕES define as vulnerabilidades de cybersegurança:

- Vulnerabilidades críticas: As vulnerabilidades de segurança da informação críticas são aquelas que representam uma ameaça imediata e de alto impacto para a organização. Isso pode incluir a exploração de falhas de segurança em sistemas de TI, como vulnerabilidades de dia zero, que permitem acesso não autorizado ou comprometimento de dados confidenciais. Para enfrentar esse tipo de vulnerabilidade, é crucial implementar medidas de segurança robustas, como firewall, criptografia, autenticação forte e monitoramento contínuo.
- Vulnerabilidades altas: As vulnerabilidades de segurança da informação de nível alto são aquelas que apresentam um risco significativo para a organização, embora possam exigir um pouco mais de esforço para serem exploradas. Isso pode incluir falhas de segurança em aplicativos web, acesso não autorizado a sistemas internos ou perda de dados devido a violações de segurança. Para mitigar essas

vulnerabilidades, é importante implementar políticas de segurança da informação, realizar testes de penetração regulares e fornecer treinamento de conscientização sobre segurança aos funcionários.

- Vulnerabilidades médias: As vulnerabilidades de segurança da informação de nível médio são aquelas que podem afetar a confidencialidade ou a integridade dos dados, mas que possuem um impacto relativamente menor em comparação com as categorias anteriores. Isso pode incluir a falta de atualizações de segurança em sistemas operacionais, práticas de senha inadequadas ou configurações incorretas de permissões de acesso. Para lidar com essas vulnerabilidades, é importante implementar políticas de gerenciamento de patches, realizar auditorias de segurança regularmente e fornecer treinamento em boas práticas de segurança aos funcionários.
- Vulnerabilidades baixas: As vulnerabilidades de segurança da informação de nível baixo são aquelas que apresentam um risco mínimo, mas ainda exigem atenção. Isso pode incluir a exposição de informações não sensíveis, como detalhes de contato, falta de backups adequados ou a presença de serviços desnecessários em sistemas. Embora o impacto dessas vulnerabilidades seja baixo, é essencial ter uma abordagem proativa, como realizar avaliações de risco regulares, manter backups atualizados e restringir o acesso a serviços desnecessários.
- Vulnerabilidades informativas: As vulnerabilidades informativas referem-se à exposição de informações que podem ser mal interpretadas ou utilizadas de forma inadequada, mesmo que não representem uma ameaça

A área de Infraestrutura e Desenvolvimento devem possuir procedimentos descritos e divulgados entre os colaboradores sobre o tratamento das vulnerabilidades encontradas em seus respectivos sistemas e equipamentos.

6.12. Gestão de Continuidade

A Monte Bravo deverá elaborar, implementar, operar, manter, controlar e melhorar continuamente a Gestão de Continuidade de Negócio, que deverá ser composto, no mínimo, pelos planos, de acordo com as suas necessidades específicas, de forma a assegurar a disponibilidade dos processos críticos de informação e a recuperação das atividades essenciais:

- Documentação dos procedimentos e informações necessárias para que a Monte Bravo mantenha seus processos de informação críticos e a continuidade de suas atividades vitais, num nível previamente definido, em casos de crises, desastres ou catástrofes.
- Documentação dos procedimentos e informações necessárias para que a Monte Bravo operacionalize o retorno das atividades críticas à normalidade.
- Os planos definidos deverão ser testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos processos críticos de informação.

6.13. Programa de Cyber Security

O programa de Cyber Security da Monte Bravo segue os princípios:

- Regulamentações vigentes;
- Melhores práticas;
- Cenários mundiais;
- Análises de risco da própria instituição
- Conforme a sua criticidade, as ações do programa dividem-se em:
- Críticas: Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
- Sustentação: Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da instituição e permitindo ações de longo prazo/estruturantes possam ser realizadas;
- Estruturantes: Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam o banco para o futuro.

6.14. Programa de Conscientização de Cyber Segurança

Abrangência: O programa de conscientização em segurança da informação tem como objetivo envolver todos os colaboradores da organização, independentemente do cargo ou nível hierárquico. Ele deve abranger tanto funcionários permanentes quanto temporários, contratados e terceirizados. Além disso, o programa pode ser estendido a parceiros de negócios e stakeholders relevantes que lidam com informações sensíveis da empresa.

Frequência: A conscientização em segurança da informação deve ser uma atividade contínua e integrada à cultura da organização. Recomenda-se realizar sessões de conscientização no momento da integração de novos funcionários, além de promover atividades periódicas ao longo do ano, como campanhas temáticas, palestras, treinamentos e boletins informativos. A frequência ideal dependerá da complexidade das informações a serem compartilhadas e da dinâmica da organização, mas é importante que a conscientização seja um esforço constante.

Aplicação: A aplicação pode ser executada em formato de integração de novos colaboradores, Treinamentos Online, Campanhas de Conscientizações, Simulações de Phishing e em diretrizes claras.

Medição: A eficácia do programa de conscientização em segurança da informação pode ser medida de várias maneiras, na forma de Testes de conhecimento, em relatórios de incidentes, avaliações de conformidade, e em pesquisas de feedbacks. É importante acompanhar regularmente as métricas e resultados obtidos, ajustando o programa conforme necessário para garantir a eficácia contínua e o engajamento dos funcionários na segurança da informação.

6.15. Tratamento de Incidentes de Segurança da Informação

Define-se como necessário as seguintes diretrizes da Monte Bravo:

- Todos os incidentes de segurança da informação notificados ou detectados deverão ser registrados, com a finalidade de assegurar o histórico das atividades desenvolvidas.
- O tratamento de incidentes de segurança da informação deverá ser realizado de forma a viabilizar e assegurar disponibilidade, integridade e confidencialidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo.
- Durante o gerenciamento de incidentes de segurança da informação, havendo indícios de ilícitos criminais, a área de Segurança da Informação, ou Departamento Pessoal, ou Departamento Jurídico, ou membros da Equipe Técnica ligadas as atividade de segurança da Informação tem como dever, sem prejuízo de suas demais atribuições, acionar as autoridades policiais competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências, exigindo consulta às orientações sobre cadeia de custódia, e priorizar a continuidade dos serviços da Monte Bravo.

6.16. Atribuições e Responsabilidades

6.16.1. Integrantes

Cabe aos integrantes da Monte Bravo cumprir com as seguintes obrigações:

- Zelar continuamente pela proteção das informações da Monte Bravo, especialmente confidencial, contra acesso, modificação, destruição ou divulgação não autorizada;
- Buscar orientação do superior imediato e/ou as áreas: Segurança da Informação, Departamento Pessoal, Jurídico, TI Corporativa (Service Desk) em caso de dúvidas relacionadas à Segurança da Informação;
- Assinar o termo de responsabilidade e confidencialidade, formalizando a ciência e o aceite das Políticas e Normas de Segurança da Informação, bem como assumindo a responsabilidade por seu cumprimento;
- Assegurar que os recursos (computacionais ou não) colocados à sua disposição sejam utilizados primariamente para fins profissionais da Monte Bravo;
- Participar dos treinamentos, palestras e apresentações, presenciais ou virtuais, de Segurança da Informação que são disponibilizados;
- Garantir que os sistemas e informações sob sua responsabilidade estejam adequadamente protegidos;
- Garantir a continuidade do processamento das informações críticas para o negócio;
- Cumprir as leis e normas que regulamentam os aspectos de propriedade intelectual;
- Atender às leis que regulamentam as atividades da empresa e seu mercado de atuação;

- Comunicar imediatamente à área de Segurança da Informação ou TI Corporativa (Service Desk) qualquer descumprimento da Política de Segurança da Informação e/ou das normas relacionadas.

6.16.2. Comitê Gestor de Segurança da Informação

O Comitê Gestor de Segurança da Informação (CGSI) é um grupo multidisciplinar que reúne representantes de diversas áreas da Monte Bravo, composto por indicados e aprovados pelas suas respectivas Diretorias, com o intuito de definir e apoiar estratégias necessárias à implantação, operação, manutenção, controle e melhoria contínua do SGSI. Assim, compete ao CGSI:

- Propor ajustes, aprimoramentos e modificações na estrutura normativa do SGSI, submetendo à avaliação da Diretoria Executiva;
- Promover a Segurança da Informação na organização, aprovando políticas de segurança da informação;
- Requisitar informações das demais áreas da organização, através das diretorias e gerências, com o intuito de verificar o cumprimento da política e normas de segurança da informação;
- Receber, analisar e notificar as gerências e diretorias, quanto a casos de violação da política e das normas de segurança da informação;
- Estabelecer mecanismos de registro e controle de eventos e incidentes de segurança da informação, bem como, de não conformidades das políticas, normas ou dos procedimentos de segurança da informação;
- Propor projetos e iniciativas relacionadas à melhoria do SGSI;
- Acompanhar o andamento dos projetos e iniciativas relacionados à segurança da informação e continuidade de negócio;
- Gerir a continuidade dos negócios, demandando junto às diversas áreas da empresa, planos de continuidade dos negócios, validando-os periodicamente;
- Realizar, sistematicamente, a gestão de riscos relacionados à segurança da informação e continuidade de negócio.

6.16.3. Diretoria (Alta Direção)

Cabe à Diretoria:

- Prover os recursos necessários para garantir a eficácia do SGSI;
- Assessorar o CGSI quanto a qualquer decisão relacionada ao sistema de gestão segurança da informação e continuidade de negócio;
- Apoiar as políticas, as diretrizes e as normas de segurança da informação e continuidade de negócio;
- Receber relatórios de violações da política, diretrizes e das normas de segurança da informação, quando aplicável;

- Receber relatórios de não conformidades dos SGSI e SGCN;
- Realizar a análise crítica do SGSI pela alta direção;
- Tomar decisões referentes aos casos de descumprimento da política, diretrizes e das normas de segurança da informação, mediante a apresentação de melhorias contínuas do SGSI.

6.16.4. Líder da área ou departamento

Cabe ao líder da área ou departamento cumprir com as seguintes obrigações:

- Cumprir e fazer cumprir a política, as normas e procedimentos de segurança da informação e continuidade de negócio;
- Assegurar que a sua equipe possua acesso e entendimento da política, das normas e dos procedimentos de Segurança da Informação e Continuidade de Negócio;
- Sugerir a Segurança da Informação ou ao CGSI, de maneira proativa, procedimentos de segurança da informação relacionados às suas áreas;
- Redigir e detalhar, tecnicamente e operacionalmente, as normas e procedimentos de segurança da informação e continuidade relacionados à sua área, quando solicitado pela Segurança da Informação;
- Comunicar imediatamente a área de Segurança da Informação eventuais casos de violação da política, de normas ou de procedimentos de segurança da informação ou continuidade de negócio.
- Incentivar que a Política, normas e procedimentos de segurança da informação e continuidade de negócio da Monte Bravo sejam cumpridos de acordo com os preceitos definidos para a sua área de atuação;
- Criar, atualizar, gerenciar os procedimentos que estão sob sua responsabilidade;
- Armazenar evidências dos processos, assim como fornecê-las quando solicitado pelas áreas de Segurança da Informação;
- Incluir na análise e elaboração de projetos internos ou com clientes, fornecedores, prestadores de serviços e parceiros de negócio, sempre que necessário e quando aplicável, avaliações específicas relacionadas à segurança da informação e continuidade de negócio, com o objetivo de proteger os interesses e ativos críticos da Monte Bravo.

6.16.5. Proprietário da Informação

O proprietário da informação é o líder do departamento ou área da Monte Bravo, considerando Diretor, Gerente, Coordenador, Líder, Supervisor ou chefe de equipe, responsável pela aprovação, revisão, orientação na classificação da informação e cancelamento de autorizações de acesso a determinado conjunto de informações sob a sua guarda.

6.16.6. Jurídico

Cabe, adicionalmente, ao Jurídico:

- Manter as áreas e departamento da Monte Bravo informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e ações envolvendo a gestão de segurança da informação e continuidade de negócio;
- Incluir na análise e elaboração de contratos de clientes, fornecedores, prestadores de serviços e parceiros de negócio, sempre que necessário e quando aplicável, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da organização;
- Avaliar, quando solicitado pelas áreas ligadas ao tema, as políticas, as diretrizes, as normas e procedimentos de segurança da informação;
- Auxiliar o CGSI e a área de Segurança da Informação nas demais questões legais.

6.16.7. Departamento Pessoal, Recursos Humanos, Treinamento e Desenvolvimento

Cabe, adicionalmente, às áreas de Recursos Humanos, Departamento Pessoal e Treinamento e Desenvolvimento:

- Assegurar-se de que os colaboradores comprovem, estar cientes da estrutura normativa do SGSI e dos documentos que a compõem, como por exemplo, o Termo de Aceite de Confidencialidade ou Responsabilidade;
- Criar mecanismos para informar, antecipadamente aos fatos, ao canal de atendimento técnico mais adequado, alterações no quadro funcional da Monte Bravo;
- Promover as campanhas de treinamento, palestras e conscientizações, via presencial ou virtual para todas as áreas e unidades da Monte Bravo;
- Obter a assinatura do Termo de Responsabilidade ou Confidencialidade dos integrantes, arquivando-o nos respectivos prontuários.

6.16.8. Segurança da Informação

Cabe à área de Segurança da Informação:

- Aprovar a composição do CGSI da Monte Bravo;
- Consolidar, manter e coordenar a elaboração e evolução, acompanhamento e avaliação do SGSI;
- Convocar, coordenar e prover apoio às reuniões do CGSI;
- Prover as informações de gestão de segurança da informação e continuidade de negócio solicitadas pelo CGSI;
- Facilitar a conscientização, a divulgação e o treinamento quanto à política, às normas e os procedimentos de segurança da informação;

- Executar projetos e iniciativas visando otimizar a segurança da informação e continuidade de negócio;
- Conduzir a Gestão, avaliação e tratamento de Risco ligados a segurança da informação e continuidade de negócio;
- Analisar, auditar e promover a Segurança da Informação, assim como, novos regulamentos, legislações e novas certificações na Monte Bravo de negócio para implementação de novos controles e requisitos dentro do escopo do SGSI;
- Criar e revisar os procedimentos de Segurança da Informação dentro do escopo do SGSI e de Continuidade de Negócios;
- Realizar rondas, vistorias, auditorias e análise crítica do escopo do SGSI, emitindo relatório para o CGSI e a alta direção;
- Atuar como ponto de orientação para outras equipes e gerências em assuntos relacionados à Segurança da Informação e Continuidade de Negócio;

7. Regulamentação e Legislação Aplicáveis

Correlacionam-se com a política, com as diretrizes e com as normas de Segurança da Informação e Continuidade de Negócio as Leis abaixo relacionadas, mas não se limitando às mesmas:

- CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988;
- CÓDIGO TRIBUTÁRIO NACIONAL pelo art. 7º do Ato Complementar nº 36, de 13.3.1967;
- CONSOLIDAÇÃO DAS LEIS DO TRABALHO -DECRETO-LEI N.º 5.452, DE 1º DE MAIO DE 1943;
- Lei Federal 10406, de 10 de janeiro de 2002 (Institui o Código Civil);
- Decreto-Lei 2848, de 7 de dezembro de 1940 (Institui o Código Penal);
- Lei Federal 9983, de 14 de julho de 2000 (Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 - Código Penal e dá outras providencias);
- LEI Nº 9.472, DE 16 DE JULHO DE 1997;
- Lei de direito autoral Nº 9610/98;
- Lei de marcas e patentes Nº 9.279 de 14/05/1996;
- Lei das telecomunicações Nº 9.472 de 16/07/1997;
- Lei de propriedade intelectual de programa de computador Nº 9.609 de 19/02/1998;
- Artigo 482 da CLT
- Lei Nº 12.737 - Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.
- Lei Nº 12.965 de 23/04/2014 (Marco Civil da Internet).

- Resolução 4.658 do Banco Central
- Resolução 4.752 do Banco Central
- Lei Nº 13.709 - Lei Geral de Proteção de Dados Pessoais
- Instrução CVM 612

8. Penalidades e Sanções

São consideradas violações à política, às diretrizes, às normas ou aos procedimentos de segurança da informação ou continuidade de negócio as seguintes situações, não se limitando às mesmas:

- Quaisquer ações ou situações que possam expor a Monte Bravo à perda financeira e de imagem, direta ou indiretamente, potenciais ou reais, comprometendo seus ativos críticos de informação;
- Utilização indevida de dados corporativos, divulgação não autorizada de informações, segredos comerciais ou outras informações confidenciais sem a permissão expressa do Líder/Proprietário da Informação;
- Uso de dados, imagens, informações, equipamentos, software, sistemas ou outros recursos tecnológicos, para propósitos ilícitos, que possam incluir a violação de leis, de regulamentos internos, como o Código de Ética, e externos, ou de exigências de organismos reguladores da área de atuação da Monte Bravo;
- A não comunicação imediata às áreas de Segurança da Informação, Departamento Pessoal, Jurídico, TI Corporativa (Service Desk) de quaisquer descumprimentos da política, dos critérios, de normas ou de procedimentos de Segurança da Informação, que porventura um colaborador venha a tomar conhecimento ou chegue a presenciar.

O não cumprimento dos itens descritos acima, ainda que por mero desconhecimento, sujeitará o infrator a sanções administrativas, incluindo, a aplicação de advertência verbal ou escrita, demissão por justa causa ou rescisão contratual, bem como sujeitará o infrator às demais penalidades administrativas, cíveis e penais previstas na legislação brasileira.

9. Disposições Finais

Esta Política de Segurança da Informação deverá ser comunicada a todos integrantes da Monte Bravo a fim de que seja cumprida dentro da organização. O não cumprimento dos requisitos previstos nesta política, nas normas complementares e nos procedimentos de Segurança da Informação ou Continuidade de Negócio, acarretará violação às regras internas da empresa e sujeitará o colaborador às medidas administrativas e legais cabíveis, podendo envolver advertência, suspensão, rescisão

contratual ou outras medidas cabíveis conforme legislação vigente, além de aplicação das punições previstas na legislação aplicável.