Brookfield

POL-001 Política de Segurança da Informação

Sumário

1. Objetivo

Estabelecer diretrizes que permitam aos Empregados e Terceiros da Empresa observarem os padrões de comportamento relacionados à segurança da Informação adequados às necessidades de negócio, de proteção legal da Empresa e do indivíduo.

Nortear a definição de normas e procedimentos específicos de segurança da Informação e orientar as condições de uso dos Recursos de TI, bem como a implementação de controles e processos para seu atendimento.

Preservar as Informações da Empresa quanto à:

- Integridade: garantia de que a Informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à Informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os Usuários autorizados obtenham acesso à Informação e aos ativos correspondentes sempre que necessário.

2. Âmbito de Aplicação

A presente norma aplica-se à Brookfield Brasil Asset Management Investimentos Ltda., à Brookfield Brasil Ltda., à BRKB Distribuidora de Títulos e Valores Mobiliários S.A. e às suas respectivas empresas controladas, sob controle comum e/ou sob sua administração, caso estas não apresentem os próprios normativos sobre o tema, cada uma delas doravante designada simplesmente por Empresa.

2.1 Algumas afiliadas da Brookfield Brasil Ltda. podem adotar políticas próprias ou complementares às disposições desta política, desde que com esta não sejam conflitantes.

2.2 A presente política abrange também Terceiros com os quais a Empresa mantenha ou venha a manter relação contratual, conforme aplicável.

3. Considerações Gerais

3.1 O conteúdo desta política é propriedade da Empresa e é destinado para uso e divulgação internos. Não pode ser reproduzido, armazenado ou transmitido, em qualquer formato ou por quaisquer meios, sejam eletrônicos ou físicos, sem prévia autorização formal do Departamento de Compliance.

3.2 Em caso de dúvidas sobre a aplicação adequada das diretrizes constantes da presente política, os Empregados devem consultar a equipe de TS, seu Gestor imediato e/ou o Departamento de Compliance.

3.3 O conteúdo desta política deve ser conhecido e observado por todos os Empregados e Terceiros da Empresa, conforme aplicável, sendo o seu descumprimento passível de aplicação das medidas legais e disciplinares mencionadas no Código de Conduta Ética da Brookfield.

3.4 A aplicação das medidas legais e disciplinares mencionadas acima não isentam, dispensam ou atenuam a responsabilidade civil, administrativa e/ou criminal, pelos prejuízos resultantes de atos dolosos ou culposos resultantes da infração da legislação em vigor, desta política, normas e procedimentos aplicáveis.

3.5 Esta política dá ciência a cada Empregado de que os ambientes, sistemas, computadores, tablets, e-mails, internet, telefones fixos e telefones móveis, redes (privada e pública), CD, DVD, e pen drive (mídias) da Empresa poderão ser monitorados e armazenados.

3.6 Os casos omissos serão decididos pelo Comitê de Ética e Integridade da Brookfield Brasil Ltda ou pelo Comitê de Privacidade e Proteção de Dados Pessoais.

3.7 O Diretor responsável pela Gestão de Recursos e o Diretor responsável pela Administração Fiduciária não deverão participar das decisões mencionadas no item 3.6 e das demais decisões relacionadas a controles internos.

4. Vínculos

Código de Conduta Ética da Brookfield
POL-007 Política de Privacidade e Proteção de Dados Pessoais
NOR-005 - Norma de Permissão de Acesso aos Sistemas

NOR-020 Norma de Telefonia Móvel
NOR-022 Norma de Acesso e Utilização dos Recursos de TI
Plano de Resposta a Incidentes

5. Conceitos

5.1 AMBIENTE DE HOMOLOGAÇÃO – Ambiente com as mesmas características do Ambiente de Produção, onde os sistemas (alterações e etc.) são testados, com objetivo de garantir que está em conformidade com tudo o que se propõe a fazer.

5.2 AMBIENTE DE PRODUÇÃO - Um ambiente controlado contendo os itens de configuração em produção usados para entregar serviços de TI.

5.3 DADO(s) PESSOAL(is) – Informação relacionada a pessoa natural identificada ou identificável, como, por exemplo, um nome, número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa natural.

5.4 DADO(s) PESSOAL(is) SENSÍVEL(is) – Dado Pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5.5 DISPOSITIVO MÓVEL – É o dispositivo de acesso remoto a qualquer dado da Empresa, incluindo, mas não se limitando à smartphone, tablet e notebook.

5.6 EMPREGADO - Refere-se a todo e qualquer conselheiro, administrador, diretor e demais funcionários da Empresa.

5.7 GESTOR - É aquele que gerencia as Informações, seu nível de confidencialidade, sua distribuição e autorizações de acesso.

5.8 INCIDENTE DE SEGURANÇA – Qualquer violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizado a Informação, Informação Confidencial e/ou Dados Pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de Tratamento.

5.9 INFORMAÇÃO - É todo e qualquer dado, informe, elemento, notícia, comunicação, material, instrução ou direção que sejam disponibilizados por escrito, oralmente ou de qualquer outra forma, gravados ou não com a expressão “confidencial”, em decorrência do desenvolvimento das atividades profissionais do Grupo Brookfield no Brasil.

5.10 INFORMAÇÃO CONFIDENCIAL - Constituem Informações Confidenciais:

a) Dados ou Informações da Empresa (ainda que não sejam de propriedade da Empresa, mas que a mesma tenha recebido em razão de uma oportunidade de negócio, por exemplo) ou desenvolvidos pela Empresa e que o Empregado venha a tomar conhecimento por qualquer forma, incluindo, mas não se limitando a, Informações de natureza técnica, comercial, financeira, jurídica, estratégica, tecnológica, know-how, desenhos, modelos, dados, cadastros, especificações, relatórios, compilações, análises, previsões, estudos, reproduções, sumários, comunicados, fórmulas, patentes, dados financeiros e econômicos, Informações relacionadas a clientes, fornecedores atuais ou potenciais, operações financeiras, planos comerciais, demonstrações ou planos financeiros, estratégias de marketing e outros negócios, contratos, produtos existentes ou futuros e quaisquer outras Informações de propriedade da Empresa ou que o Empregado tenha acesso;

b) Outros dados ou Informações necessárias para o exercício das funções do Empregado relativos à Empresa, incluindo, mas não se limitando a, dados de natureza societária, objetivos de investimentos, estrutura jurídica e segredos de negócio; e

c) Todas as anotações, análises, compilações, estudos, materiais ou quaisquer outros documentos elaborados pela Empresa e/ou por seus Empregados, representantes, prepostos, consultores jurídicos, consultores contábeis, consultores financeiros, auditores internos e independentes, que contenham ou reflitam de outra maneira Informações da Empresa.

5.11 MATERIAL DE CONTEÚDO INADEQUADO – É considerado como inadequado, qualquer arquivo digital, que possua, por exemplo, um ou mais dos conteúdos enquadrados na lista abaixo:

a) Ilícitos, conteúdos violentos ou degradantes;

b) Protegido por direitos autorais, segredo comercial, industrial ou de Terceiros, a menos que o Usuário tenha permissão do titular de tais direitos para divulgar o conteúdo;

c) Nocivo, abusivo, difamatório, pornográfico, libidinoso ou que de qualquer forma represente assédio, invasão de privacidade ou risco a menores;

d) Que represente assédio, degradação, intimidação ou ódio em relação a um indivíduo ou grupo de indivíduos com base na religião, sexo, orientação sexual, raça, origem ética, idade, deficiência, ou qualquer outra condição;

e) Que inclua informações pessoais ou que permitam a identificação de Terceiro sem seu expresso consentimento;

f) Falso, fraudulento, enganoso ou que represente informação enganosa;

g) Que contenha referência a link ilícito, spam, correntes ou esquemas de pirâmide; e

h) Que contenha vírus ou qualquer outro código malicioso, arquivos ou programas projetados para interromper, destruir ou limitar a funcionalidade de qualquer software ou hardware.

5.12 RECURSOS DE TECNOLOGIA DA INFORMAÇÃO (TI) - São ferramentas de tecnologia da informação disponibilizadas ao Empregado para utilização a serviço da Empresa, tais como, mas não se limitando a: internet, intranet, rede corporativa com seus respectivos diretórios, correio eletrônico (e-mail), Dispositivos Móveis, computadores, pen-drives, impressoras, scanners, softwares e sistemas aplicativos.

5.13 SERVIÇOS DE TECNOLOGIA (TS) – grupo responsável por oferecer, manter e suportar serviços e Recursos de TI.

5.14 TECNOLOGIA DA INFORMAÇÃO (TI) – Conjunto de todas as atividades e soluções providas por recursos de computação que visam permitir o processamento, armazenamento, acesso e uso das Informações.

5.15 TERCEIRO - Refere-se, mas não se limitando, a todo e qualquer prestador de serviços, fornecedor, consultor, cliente, parceiro de negócio, terceiro contratado ou subcontratado, locatário, cessionário de espaço comercial, sejam pessoas físicas ou jurídicas, independentemente de contrato formal ou não, incluindo aquele que utiliza o nome da Empresa para qualquer fim ou que presta serviços, fornece materiais, interage com o governo ou com outros em nome da Empresa no âmbito do contrato.

5.16 TRATAMENTO – Toda operação realizada com Dados Pessoais ou não, como, por exemplo, as que se referem 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.

5.17 UPLOAD – Ato de enviar um arquivo para a internet, ou seja, envio de dados de um computador local para um computador remoto, fora da rede corporativa.

5.18 USUÁRIO - É todo e qualquer Empregado, Terceiro ou visitante que utilize os Recursos de TI disponibilizados pela Empresa.

6. Diretrizes

6.1 Gerais

a) Toda Informação, Confidencial ou não, é propriedade da Empresa, ressalvadas aquelas Informações Confidenciais de propriedade de Terceiros que sejam obtidas pela Empresa através de um acordo de confidencialidade ou documento equivalente. São ativos corporativos valiosos que devem ser gerenciados com o devido cuidado.

b) Todos os Dados Pessoais e/ou Dados Pessoais Sensíveis devem ser protegidos contra o Tratamento não autorizado ou ilegal e de situações acidentais a fim de prevenir a ocorrência de Incidentes de Segurança.

c) Os Dados Pessoais, Dados Pessoais Sensíveis e as Informações da Empresa devem ser usadas exclusivamente para fins empresariais.

d) Não é permitida a cópia de Dados Pessoais, Dados Pessoais Sensíveis e de Informações da Empresa sem prévia autorização expressa.

e) É responsabilidade de todos os Empregados o descarte correto de mídias, devendo sempre utilizar fragmentador ou outro método para inutilizar o acesso às Informações, aos Dados Pessoais e/ou Dados Pessoais Sensíveis nelas contidas.

f) Informações enviadas a Terceiros devem ser transportadas por portador autorizado e em envelope lacrado ou transmitidas de forma segura.

g) Os procedimentos e controles para envio de Dados Pessoais a Terceiros estão definidos na POL-007 Política de Privacidade e Proteção de Dados Pessoais.

h) É dever de todos os Empregados e Terceiros da Empresa:

- Proteger e salvaguardar os ativos da Empresa de perda, roubo, mau uso e desperdício;
- Proteger o sigilo dos Dados Pessoais, Dados Pessoais Sensíveis e de Informações Confidenciais e não públicas de propriedade da Empresa e Terceiros;
- Tomar todas as medidas razoáveis para garantir a segurança de cópias dos Dados Pessoais, Dados Pessoais Sensíveis e de Informações Confidenciais; e
- Ter discrição ao falar sobre assuntos envolvendo a Empresa em locais públicos, tais como elevadores, restaurantes, aviões ou ao utilizar seu telefone ou e-mail fora do escritório.

i) Dados Pessoais, Dados Pessoais Sensíveis e as Informações Confidenciais não podem ser deixadas em locais com acesso irrestrito, como o diretório "*Public*" do servidor de arquivos da rede de dados, ou ainda como a recepção, copa e/ou salas de reunião da Empresa. Também deverá ser dispensada atenção no momento da impressão, envio e descarte dessas Informações.

j) É imprescindível tomar os devidos cuidados com o manuseio, transmissão oral e escrita de Dados Pessoais, Dados Pessoais Sensíveis e de Informações Confidenciais.

k) Cabe ao Gestor tomar todos os cuidados para que Dados Pessoais, Dados Pessoais Sensíveis e Informações Confidencias não estejam acessíveis para pessoas não autorizadas.

l) O Gestor de cada departamento é o responsável pelos Dados Pessoais, Dados Pessoais Sensíveis e Informações Confidenciais nele produzidas e pela autorização do acesso dos Usuários à estes Dados Pessoais e informações, bem como a guarda em local restrito ou em base de dados eletrônica conforme recursos disponibilizados pelo equipe de TS para tal.

m) Não deve ser mantido nenhum Dado Pessoal, Dado Pessoal Sensível, Informação, arquivo ou dado corporativo em discos locais dos computadores corporativos ou qualquer outro meio de armazenamento senão aqueles disponibilizados pela equipe de TS (Servidor de Arquivos, OneDrive, Sharepoint e outras soluções de colaboração)

n) Quaisquer mudanças nos processos e rotinas da Empresa devem ser realizadas em conformidade com esta política.

o) Os Empregados devem zelar para que Material de Conteúdo Inadequado não seja exposto, armazenado, distribuído, editado ou gravado.

p) Visando a proteção das Informações da Empresa de ataques maliciosos, a equipe de TS global mantém ativas ferramentas de controle de tráfego da internet, filtragem de e-mails e de isolamento/restrição de acesso as suas redes internas.

q) É terminantemente proibido fazer, divulgar ou compartilhar comentários, mensagens ou discussões sobre a Empresa, seus clientes, e seus investidores, Dados Pessoais, Dados Pessoais Sensíveis e Informações referentes a qualquer estratégia, inclusive de investimento, feitas através de redes sociais, salas de bate-papo, wikis, mundos virtuais e blogs (Mídias Sociais), a menos que expressamente autorizado pela área de comunicações e relações com investidores.

r) Os arquivos contidos na pasta pública do servidor de arquivos são para utilização temporária e serão excluídos pela equipe local de TS periodicamente.

s) Ao utilizar os meios de comunicação e ferramentas de trabalho disponibilizados pela Empresa, não espere que as Informações enviadas ou recebidas serão privadas. Sua atividade poderá ser monitorada e armazenada a fim de garantir que esses recursos sejam utilizados de forma adequada.

t) Os computadores corporativos (desktops e notebooks) possuem criptografia da unidade de disco, que visa impedir que usuários não autorizados violem a proteção dos dados em computadores perdidos, roubados ou desativados de maneira inadequada. A criptografia tem por objetivo garantir que os arquivos do sistema operacional somente poderão ser acessados por Usuários autorizados.

u) A cada dois anos a equipe local de TS realizará testes de segurança para os sistemas de Informação.

v) A equipe de TS realizará periodicamente campanhas de conscientização, programas de capacitação e avaliação periódica relacionada a Segurança da Informação para os Empregados.

6.2 Áreas de Acesso Restrito

a) As áreas de negócios ou operações da Empresa devem, preferencialmente, restringir o acesso físico. Ficam estabelecidas as seguintes áreas de acesso restrito:

- Centros de Processamento de Dados (“CPD”); e
- Sala de Elétrica.

b) Somente funcionários de TI ou pessoas autorizadas pelo Departamento podem ter acesso aos CPDs da Empresa.

6.3 Recursos de TI

a) As diretrizes, responsabilidades e procedimentos a serem observados em relação ao acesso e utilização dos Recursos de TI são definidas e estão disponíveis na NOR-022 Norma de Acesso e Utilização dos Recursos de TI.

b) As permissões de acesso aos Recursos de TI da Empresa devem ser baseadas nas necessidades de negócio, considerando-se o perfil funcional dos Usuários.

c) É responsabilidade de cada Gestor a solicitação formal de liberação, alteração, suspensão ou revogação de acesso dos Empregados e Terceiros de sua equipe a qualquer recurso de TI.

d) A fim de haver um controle quanto aos privilégios de acesso dos Usuários, qualquer afastamento, seja temporário ou permanente, incluindo a mudança de departamento de atuação, deverá ser informado, formalmente pelos Gestores dos departamentos envolvidos, para que sejam tomadas as medidas cabíveis quanto ao cancelamento ou suspensão provisória e permissão do acesso.

e) Toda solicitação de acesso aos Recursos de TI deverá ser documentada formalmente e justificada quanto à sua real necessidade.

f) Os acessos concedidos a Terceiros deverão ter caráter provisório sendo obrigatório ao Gestor responsável pelo mesmo indicar, no ato da solicitação, o prazo limite para utilização dos recursos e a data de encerramento do contrato com o Terceiro.

g) Todo equipamento de TI deve ser homologado pela equipe de TS.

h) Apenas os Empregados de TI ou pessoas autorizadas pela equipe de TS podem realizar a instalação e/ou desinstalação, assim como a parametrização, de hardware e/ou software dos equipamentos corporativos.

i) O Usuário é o responsável pela conservação e integridade dos Recursos de TI que utiliza. Cuidados como desligar o computador, inclusive o monitor, ao final do dia e não manter líquidos próximo aos equipamentos são fundamentais para garantir que a vida útil dos mesmos não seja reduzida.

j) O Usuário para o qual for disponibilizado notebook e/ou telefone móvel corporativo deverá assinar o Termo de Responsabilidade específico para estes equipamentos.

k) Nenhum Usuário pode utilizar os recursos da Empresa para deliberadamente propagar qualquer tipo de vírus, worm, spam ou programas de controle de outros computadores.

l) Nenhum Usuário pode utilizar os recursos da Empresa para fazer o download ou distribuição de software não licenciado. Da mesma forma, não é permitido efetuar Upload de qualquer software licenciado à Empresa ou de dados de propriedade desta ou de seus clientes, sem expressa autorização do Gestor responsável pelo software ou pelos dados.

m) A equipe de TS poderá disponibilizar acesso remoto aos sistemas e e-mails corporativos como uma facilidade aos Empregados.

n) O Empregado que utilizar telefone móvel próprio para acesso aos sistemas e e-mails da Empresa deverá observar também a NOR-020 Norma de Telefonia Móvel.

6.4 Gerência de Usuário e Senha

a) A identificação de acesso aos Recursos de TI deve ser efetuada através de uma senha, pessoal e intransferível, criada pelo próprio Usuário, mediante a observância de regras básicas que visem a garantir a segurança do acesso e da utilização dos recursos, sendo proibido o seu compartilhamento.

b) O Usuário é responsável por zelar pela confidencialidade e sigilo de suas senhas e logins.

c) Ações realizadas com identificação e senhas do Usuário, como manuseio de dados em arquivos, planilhas eletrônicas e/ou sistemas, serão de inteira e exclusiva responsabilidade do Usuário.

d) Para evitar o acesso indevido de outras pessoas aos Recursos de TI, o Usuário deve desligar o computador ou efetuar o bloqueio (CTRL + ALT + DEL + ENTER) sempre que se afastar do equipamento.

e) Os Usuários que utilizam Dispositivos Móveis deverão obrigatoriamente manter a senha de seus dispositivos habilitada e a equipe local de TS poderá utilizar ferramentas que assegurem isso.

f) O uso de dispositivos e/ou senhas de identificação de outra pessoa é terminantemente proibido e está sujeito às penalidades aplicáveis. Assim, nenhum dispositivo de identificação poderá ser compartilhado, em nenhuma hipótese.

g) Mecanismos automáticos implantados pela equipe de TS bloqueiam as contas de Usuários após tentativas de acesso com senha incorreta. Para solicitar o desbloqueio busque orientações junto a equipe de TS.

h) Mecanismos automáticos implantados pelo Departamento de TI asseguram a alteração periódica de senha dos Usuários, porém os Usuários podem alterar a própria senha a qualquer momento que desejarem.

6.5 Internet

a) A internet disponibilizada pela Empresa deverá ser utilizada preferencialmente para fins profissionais. Essa regra se estende as redes wi-fi da Empresa.

b) É proibido acessar, nos Recursos de TI e demais ferramentas disponibilizadas pela Empresa, as seguintes categorias de sites: apostas, propaganda, adultos, com material obsceno/ofensivo, atividades criminais/ilícitas, armas, violência, expressões de ódio, encontros, jogos, bate-papo (chat), sites que façam ou permitam controle remoto de computadores, hacking, sites com transmissão de som e vídeo que não sejam para fins profissionais, e outras que vierem a ser bloqueadas.

c) As regras mencionadas nesta política para uso dos Dispositivos Móveis devem ser respeitadas também quando utilizados fora da Empresa.

6.6 E-mail e sistemas de mensagens instantâneas

a) O e-mail corporativo deverá ser utilizado exclusivamente para fins de negócio.

b) Todos os assuntos de negócios devem ser conduzidos pelo sistema de correio eletrônico (e-mail) da Empresa e ou por sistemas de mensagens homologados pelo Departamento de TI. Não devem ser utilizadas contas de e-mail pessoal, SMS, MMS ou qualquer serviço de mensagens instantâneas e sites de mídia social.

c) O Departamento de TI fixará limites quanto ao tamanho das caixas postais, volume total de mensagens enviadas, quantidade de mensagens armazenadas nos servidores de e-mail, número de destinatários, tamanho e tipo de anexos e tamanho de cada mensagem enviada com a finalidade de garantir o bom funcionamento do serviço de acordo com os recursos disponibilizados, segurança e confidencialidade.

d) A qualquer momento que julgar necessário, o Departamento de TI pode utilizar mecanismos para bloqueio, na entrada ou saída de mensagens, por tamanho, por anexos e download de arquivos que não sejam condizentes com as atividades da Empresa.

6.7 Gerência de Antivírus

Com o objetivo de proteger arquivos e Informações eletrônicas da Empresa de vírus eletrônicos, a equipe global de TS deve manter atualizada a ferramenta de controle de prevenção e detecção desses vírus, respeitando no mínimo a periodicidade recomendada pelo fabricante.

6.8 Sistemas de Informação

a) Cabe a equipe de TS homologar soluções técnicas e aos Usuários homologar as funcionalidades dos sistemas.

b) As solicitações para desenvolvimento ou contratação de novos sistemas devem ser encaminhadas a equipe local de TS, que deverá observar as melhores práticas de Segurança da Informação.

c) Os Ambientes de Homologação e Produção são segregados, garantindo assim, a integridade dos dados.

d) A Empresa deve, através de seus Gestores, estabelecer prazos e procedimentos para arquivamento e descarte de Informações, Dados Pessoais e Dados Pessoais Sensíveis, cumprindo com os requisitos legais e regulamentares aplicáveis.

e) Todos os programas instalados são registrados, homologados e licenciados, não sendo permitido ao Usuário:

- Instalar qualquer tipo de software não autorizado pela equipe de TS; e
- Desativar ou mudar a configuração e/ou parametrização dos programas instalados nos equipamentos disponibilizados.

f) A reprodução não autorizada dos softwares instalados nos equipamentos disponibilizados constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

6.9 Respostas a Incidentes

Os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes relevantes de Dados Pessoais, Dados Sensíveis e Informações Corporativas estão definidos no Plano de Resposta a Incidentes.

6.10 Notificação e Investigação de Suspeitas de Violação

Os Empregados devem ser proativos e denunciar prontamente qualquer suspeita de violação desta Política conforme diretrizes do Código de Conduta Ética da Brookfield.

7. Disposições Finais

Esta política entrará em vigor na data de sua divulgação, revogando e substituindo qualquer comunicação anterior sobre o assunto.

8. Controle e Histórico de Versões

Data	Versão	Sumário
01/06/2006	01/2006	Criação do instrumento normativo
17/08/2010	01/2010	1ª Revisão do instrumento normativo
02/07/2014	01/2014	2ª Revisão do instrumento normativo
02/07/2015	01/2015	Revisão anual do instrumento normativo
30/06/2016	01/2016	Revisão anual do instrumento normativo

06/07/2017	01/2017	Revisão anual do instrumento normativo
13/07/2018	01/2018	Revisão anual do instrumento normativo
17/07/2019	01/2019	Revisão anual do instrumento normativo
14/09/2020	01/2020	Revisão anual do instrumento normativo
04/10/2021	01/2021	Revisão anual do instrumento normativo
10/03/2023	01/2023	Revisão anual do instrumento normativo

9. Aprovações

Código	Descrição	Versão	Vigência
POL-001	Política de Segurança da Informação	01/2022	10/03/2023 a 10/03/2024

Emissor(es): Rodrigo Reis (aprovado eletronicamente em 21/12/2023)

Revisor(es): Matheus Leonel/ Felipe Carneiro (aprovado eletronicamente em 09/01/2023 e em 21/12/2022)
Aprovador(es):

Henrique Martins (aprovado eletronicamente em 21/03/2023)
Paulo Garcia (aprovado eletronicamente em 06/03/2023)
Luiz Ildefonso (aprovado eletronicamente em 06/03/2023)
Esteban Fornasar (aprovado eletronicamente em 06/03/2023)
Isacson Casiuch (aprovado eletronicamente em 07/03/2023)
Sandro Januzzi (aprovado eletronicamente em 07/03/2023)