

**INTER CONSTRUTORA E INCORPORADORA S.A.**

*Companhia Aberta*

CNPJ 09.611.768/0001-76

NIRE 31.300.117.898

**ATA DA REUNIÃO DO CONSELHO DE ADMINISTRAÇÃO**

- 1. Data, Hora e Local:** realizada em 31 de maio de 2021, às 14:15 horas, realizada na forma exclusivamente digital por meio da plataforma digital *Microsoft Teams* (“Plataforma Digital”).
- 2. Convocação:** Dispensada a convocação, dada a presença da totalidade dos seus membros, na forma do parágrafo 2º, do artigo 16, do Estatuto Social da Inter Construtora e Incorporadora S/A (“Companhia”).
- 3. Presença:** Todos os membros do Conselho de Administração estavam presentes e participaram por videoconferência, conforme parágrafo 3º, do artigo 16, do Estatuto Social da Companhia. Estava presente, também, o Diretor Financeiro e de Relação com Investidores da Companhia, Sr. Matheus de Ávila Ferreira Torga.
- 4. Composição da Mesa:** Presidente: Nair Veras Saldanha; Secretário: Flávio de Almeida Vale.

**Ordem do dia:** (I) Deliberar sobre: (i) a eleição do Diretor Vice-Presidente e do Diretor de Engenharia, tendo em vista a criação dos respectivos cargos na Assembleia Geral Ordinária e Extraordinária da Companhia realizada em 30 de abril de 2021; (ii) a revisão do Código de Ética e Conduta da Companhia; (iii) as Políticas de Anticorrupção, Transação com Partes Relacionadas, Segurança da Informação e de Resposta a Incidentes de Segurança da Informação; (iv) a concessão de autorização para que a Diretoria da Companhia tome as medidas necessárias visando à consecução das deliberações constantes da ordem do dia; (II) Apresentação do Diretor Financeiro da Companhia sobre (a) os resultados do período de três meses findo em 31 de março de 2021 e a prévia das informações financeiras do mês de abril de 2021, (b) atualização do status de adequação da Companhia à Lei Geral de Proteção de Dados (“LGPD”), e (c) atualização do status da negociação do instrumento de dívida a ser emitido no mercado de capitais, como debenture, Certificado de Recebível Imobiliário (“CRI”) ou instrumento equivalente, no valor de até R\$75.000.000,00 (setenta e cinco milhões de reais), com objetivo de: (a) repagamento de dívidas de curto prazo; (b) alongar o perfil de vencimento das dívidas da Companhia; e (c) reforço de caixa;

- 5. Deliberações:** Após análise e discussão das matérias da ordem do dia, os conselheiros presentes decidiram por unanimidade e sem restrições:

- (i) eleger **(a) o Sr. Ednilson de Oliveira Almeida**, brasileiro, administrador de empresas, casado, inscrito no Cadastro de Pessoas Físicas do Ministério da Economia (“CPF/ME”) sob o nº 043.631.716-85, com endereço na cidade de Juiz de Fora, Estado de Minas Gerais, para o cargo de **Diretor Vice-Presidente**; **(b) o Sr. Gladson Apolinário**, brasileiro, engenheiro civil, inscrito no CPF/ME sob o nº 309.787.266-34, com endereço na cidade de Juiz de Fora, Estado de Minas Gerais, para o **Cargo de Diretor de Engenharia**.

Os novos Diretores da Companhia, após investidos em seus cargos, deverão neles permanecer até a reunião do Conselho de Administração, subsequente à assembleia geral ordinária da Companhia que deliberar sobre as demonstrações financeiras referentes ao exercício social encerrado em 31 de dezembro de 2021, e que deliberar sobre a eleição da Diretoria para o mandato seguinte.

Com base nas informações recebidas pela administração da Companhia, nos termos da legislação aplicável, foi informado aos Conselheiros que os diretores ora eleitos preenchem os requisitos previstos na Lei nº 6.404, de 15 de dezembro de 1976, conforme alterada (“Lei das S.A.”) e estão em condições de firmar, sem qualquer ressalva, a declaração mencionada no artigo 147 da referida lei, e no artigo 2º da Instrução CVM 367/02. Os Diretores tomarão posse nos referidos cargos no prazo de até 30 (trinta) dias contados da presente data, mediante assinatura do respectivo termo de posse a ser lavrado em livro próprio da Companhia acompanhado da declaração de desimpedimento mencionada acima.

Na forma do Parágrafo 8º, do artigo 20, do Estatuto Social da Companhia, o Diretor Presidente, Sr. Neylson de Oliveira Almeida, acumulará as funções dos cargos até que os Srs. Ednilson de Oliveira Almeida e Gladson Apolinário tomem posse nos referidos cargos;

- (ii) aprovar o Código de Ética e Conduta da Companhia;
- (iii) aprovar as Políticas de Anticorrupção, de Transação com Partes Relacionadas, de Segurança da Informação e de Resposta a Incidentes de Segurança da Informação;
- (iv) conceder autorização para que a Diretoria da Companhia tome as medidas necessárias visando à consecução dos itens constantes da ordem do dia.

Após, o Diretor Financeiro realizou apresentação sobre as matérias indicadas no item II da ordem do dia acima, as quais foram debatidas por todos, tendo sido esclarecidos todos os questionamentos realizados.

**6. Encerramento:** Nada mais havendo a tratar, foram encerrados os trabalhos, lavrando-se a presente ata, a qual foi lida e aprovada por todos, tendo sido assinada pelos Conselheiros e Membros da Mesa presentes.

Juiz de Fora, 31 de maio de 2021

**Nair Veras Saldanha**

Presidente da Mesa

**Flávio de Almeida Vale**

Secretário

Conselheiros:

Nair Veras Saldanha

Presidente do Conselho de Administração

Jurandir Miguel de Lima

Ednilson de Oliveira Almeida

Fábio Borges Mirandez

Wilson Bernardes Alves

# CÓDIGO DE ÉTICA E CONDUTA

---

GRUPO INTER



## Mensagem do Presidente

Caro (a) leitor (a),

A Inter Construtora e Incorporadora S.A. (“**Companhia**”) começou suas atividades na cidade de Juiz de Fora, em 2008, e desde então, princípios como ética, integridade e transparência permeiam todas as nossas relações e ações. Com base nesses valores, apresentamos a nova versão do nosso Código de Ética e Conduta, o qual será o direcionador das nossas atuações internas e externas.

Este Código é um grande aliado na disseminação da nossa cultura de fazer o certo em qualquer situação, buscando sempre as melhores práticas de mercado e adoção de uma gestão de excelência, focados no crescimento e consolidação da Companhia.

Contamos com o apoio de todos os nossos colaboradores, fornecedores, parceiros, clientes, investidores e acionistas para que todas as diretrizes deste Código sejam praticadas perenemente. Por isso, é extremamente importante que todos leiam e compreendam as regras aqui estabelecidas.

O nosso objetivo é criar um ambiente de trabalho onde todos se sintam bem, pautado em relações respeitadas, humanas e saudáveis. Para tanto, a responsabilidade de fazer o certo é de cada um.

Conto com o seu apoio!

Cordialmente,

(Assinatura Neylson)

## Sumário

Mensagem do Presidente .....	1
1. Introdução .....	4
Missão .....	4
Visão .....	4
Valores.....	4
2. Princípios Éticos.....	5
Comitê de Auditoria .....	5
Canal Confidencial.....	6
Medidas Disciplinares .....	6
Treinamentos periódicos .....	7
Cumprimento da Legislação.....	7
Repúdio a mão de obra escrava e infantil.....	7
Indicação e contratação de familiares de colaboradores .....	7
Brindes e presentes.....	8
Eventos de negócio .....	8
3. Princípios de Conduta .....	8
Ambiente de trabalho .....	9
Qualidade, Segurança, Meio Ambiente e Saúde.....	9
Redes Sociais .....	10
Conflito de Interesse .....	10
Recursos e Ativos .....	11
Confidencialidade.....	11
4. Ações Institucionais.....	12
Doações e Patrocínios .....	12
Corrupção e Lavagem de Dinheiro.....	12
Acurácia nos registros contábeis.....	13
5. Relacionamentos.....	13
Clientes.....	13
Fornecedores, prestadores de serviços e parceiros.....	13
Empreiteiros .....	14
Investidores e acionistas .....	15
Setor Público .....	15
Imobiliárias e profissionais associados.....	16
Sindicatos .....	16
Mídias .....	16
Concorrência .....	16

6. Termo de ciência e compromisso ..... 17

## 1. Introdução

Desde a sua fundação, a Companhia é reconhecida, principalmente, pela qualidade, velocidade e cumprimento daquilo que é firmado em contrato com os seus clientes. “Cumprir o combinado” é um dos principais alicerces da empresa, um valor que ela não abre mão de ser seguido.

Para continuar sendo a preferida por seus clientes, crescer com sustentabilidade e ganhar novos mercados, a Companhia criou, ao final de 2019, a primeira versão de seu Código de Conduta. No referido documento, constam a missão, valores e princípios que orientam as ações de seus colaboradores e explicitam a postura da Companhia, suas controladas e controladores (“**Grupo Inter**”) em face dos diferentes públicos com os quais interage.

No momento em que o Grupo Inter decidiu expandir suas operações, vislumbrando novas oportunidades e o aumento do número de projetos em execução, fez-se necessário rever e tornar ainda mais claros certos valores, os quais deverão ser seguidos e obedecidos por todos com os quais a empresa se relaciona: colaboradores, fornecedores, parceiros, clientes, investidores e acionistas, governos e comunidades onde atua. O crescimento e expansão da Companhia reforça ainda mais a necessidade de intensificar os princípios praticados e defendidos pelos acionistas fundadores, os quais permanecem norteando toda a empresa na condução de um negócio sustentável, íntegro, ético e transparente.

Esta é, portanto, a nova versão do Código de Ética e Conduta do Grupo Inter, atualizada e aprovada pelo Conselho de Administração da Companhia em **31 de maio** de 2021. O documento tem validade por tempo indeterminado e todos aqueles que se relacionam com o Grupo, quais sejam colaborador, fornecedor, parceiro, cliente, acionista e investidor, devem conhecer as diretrizes e obrigações aqui contidas.

Todas as definições, conceitos, regras e políticas contidas no referido Código deverão ser rigorosamente observadas. Este documento deverá ser utilizado como referência para orientar a conduta, ações e decisões de todos, visando sempre preservar a credibilidade das nossas empresas. Queremos que todos aqueles que transacionem com o Grupo Inter tenham a certeza de que vamos “cumprir o combinado”.

### Missão

Desenvolver e construir habitação a um custo baixo.

### Visão

Expandir com agilidade, mantendo a qualidade e a rentabilidade.

### Valores

### Ética

Somos íntegros na condução do nosso negócio e fazemos sempre o que é certo.

### União e respeito

Unimo-nos como um time e agimos como “donos”. Tratamos todos os que interagem com o Grupo Inter, seja nas relações internas ou externas, com igualdade, confiança, lealdade e justiça. Reconhecemos e aceitamos as diferenças inerentes à diversidade das relações, as quais são pautadas por respeito absoluto ao ser humano.

### Meritocracia

Buscamos resultados diferenciados e gostamos de ser reconhecidos por isso. Dessa forma, não toleramos subdesempenho satisfatório. Valorizamos, retemos e investimos nos colaboradores com desempenho diferenciado.

### Excelência

Desempenhamos todas as nossas atividades com padrões superiores de qualidade e em constante inovação, a partir de um ambiente em que o entusiasmo, a vontade de aprender e ensinar, o comprometimento e a postura profissional são exemplares e contagiantes.

### Agilidade

Prezamos pela agilidade em todas as nossas ações, pautados pela ética e boa conduta para com todos, colaboradores, parceiros, fornecedores, clientes, investidores e acionistas, mantendo o comprometimento de cumprir o que combinamos.

## 2. Princípios Éticos

### Comitê Transitório

É dever de todos cuidar da perenidade do Grupo Inter, assegurando a aplicabilidade e a aderência do Código de Ética e Conduta.

As situações não previstas neste código e/ou situações de descumprimento dele, desde que exijam alto grau de independência e/ou conflitam com a gestão, serão levadas para avaliação de um Comitê Transitório, o qual definirá as ações a serem tomadas. As demais situações, não enquadradas neste contexto, serão avaliadas e definidas pela Diretoria Executiva.

O Comitê Transitório será formado por um representante do Conselho de Administração, um representante da Diretoria Executiva, um representante da área de Governança, Riscos, Compliance e Privacidade e um representante do Jurídico, sendo vedada a participação de membros conflitados, a serem indicados, sob demanda, pelo Diretor Presidente ou, na ausência ou impedimento dele, pelo Diretor Vice-Presidente ou, na ausência ou impedimento de ambos, pelo Conselho de Administração da Companhia, com a abstenção de voto dos membros

impedidos, conforme aplicável. São deveres da área responsável pela governança, riscos e compliance:

- . Fiscalizar e exigir o cumprimento deste Código de Ética e Conduta;
- . Propor atualizações neste código, sempre que necessário, mediante aprovação do Conselho de Administração;
- . Submeter, ao Comitê Transitório, as situações não previstas neste código e/ou situações de descumprimento dele, quando se tratar de situações que exijam alto grau de independência e/ou conflitam com a gestão, e à Diretoria Executiva, as situações que não se enquadram neste contexto.

### Canal Confidencial

Qualquer ato ou indício de ato que viole este Código de Ética e Conduta, bem como infrações ou desconformidades com as políticas, procedimentos e regulamentos internos do Grupo Inter e da legislação vigente, deverão ser relatados, assegurando a proteção dos padrões éticos adotados pelo Grupo e preservando sua imagem no mercado.

Qualquer pessoa que não se sinta confortável e seguro para relatar algum fato que esteja lhe causando incômodo ou desconfiança, poderá optar por realizar uma denúncia, identificada ou anônima, por meio do nosso Canal Confidencial.

Site: <https://interconstrutora.legaletica.com.br/>

Telefone: 0800 400 3333

E-mail: [interconstrutora@legaletica.com.br](mailto:interconstrutora@legaletica.com.br)

Nosso Canal Confidencial é operado por uma empresa terceirizada especializada no recebimento de denúncias de forma confidencial e com preservação do anonimato. Embora não seja necessária a identificação do denunciante, é fundamental agir com responsabilidade ao efetuar um relato, que deve ser consistente e verídico.

O anonimato é garantido e o Grupo Inter não admite qualquer forma de retaliação, discriminação ou sanção contra qualquer indivíduo que exponha uma preocupação verdadeira e de boa fé. Além disso, a Companhia se compromete à ampla proteção contra retaliações aqueles que decidirem utilizar o canal confidencial.

### Medidas Disciplinares

Toda denúncia será objeto de investigação imediata, guiada por processos íntegros, éticos e seguros.

Após o processo de investigação, caso seja constatada a má conduta, medidas corretivas serão imediatamente adotadas e aplicadas de maneira exemplar, sempre de acordo com as circunstâncias, gravidade e lei aplicável.

Qualquer das partes que viole o disposto neste Código estará sujeito às sanções disciplinares listadas abaixo:

- . Advertência oral;
- . Advertência por escrito;
- . Suspensão de contrato;
- . Demissão sem justa causa;
- . Demissão por justa causa;
- . Exclusão do fornecedor, parceiro ou agente intermediário do Grupo Inter;
- . Ação judicial cabível.

### Treinamentos periódicos

Além da assinatura do Termo de Ciência e Compromisso, no momento da admissão, o conteúdo deste Código de Ética e Conduta será levado ao conhecimento de todos os colaboradores do Grupo Inter por meio de treinamentos periódicos e materiais informativos.

### Cumprimento da Legislação

O Grupo Inter se compromete a cumprir e exigir o cumprimento da legislação aplicável, destacando-se as leis anticorrupção brasileiras, em especial a Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e a Lei Anticorrupção, nº 12.846/13, estando obrigado a cumpri-las integralmente e abster-se de praticar qualquer ação que viole leis e regulamentos vigentes.

### Repúdio a mão de obra escrava e infantil

O Grupo Inter não tolera e repudia, absolutamente, a utilização de mão de obra escrava e infantil ou qualquer outra forma de exploração que agrida a dignidade humana, dentro ou fora da empresa.

### Indicação e contratação de familiares de colaboradores

A admissão ou contratação de parentes ou pessoas relacionadas afetivamente com colaboradores é permitida pelo Grupo Inter, desde que observados as seguintes situações:

- . A relação deverá ser comunicada antes da admissão ou contratação;
- . O candidato deverá percorrer todo o processo seletivo, sem favorecimento, privilégio ou informação antecipada;
- . É proibida a contratação de familiares e/ou pessoas relacionadas afetivamente na mesma linha de reporte hierárquico, seja direto ou indireto;

. É proibido manter relacionamento afetivo com subordinado direto ou indireto.

Qualquer dúvida sobre um possível conflito de interesses deverá ser reportado à área responsável pela governança, riscos e compliance.

### Brindes e presentes

O recebimento e a oferta de brindes e presentes não podem ser utilizados como forma de influenciar qualquer decisão de negócio.

O recebimento somente poderá acontecer com a finalidade de atender às funções de lembrança da marca e/ou agradecimento. Ainda assim, deverão ser institucionais, tais como materiais de escritório e souvenirs, e sem valor de mercado.

No caso de recebimento de brindes e presentes diferentes dos supracitados, só poderão ser aceitos se declarados à Comunicação Interna (RH) para realização de sorteio entre os colaboradores ou para serem destinados a premiações internas. Quaisquer outros tipos de benefícios ou vantagens, incluindo viagens e hospedagens, deverão ser recusados. Especificamente almoços e jantares poderão ser aceitos, desde que não sejam recorrentes.

Da mesma forma, nós somente podemos ofertar brindes e presentes institucionais, desenvolvidos como parte da estratégia de comunicação do Grupo Inter, a clientes, fornecedores, parceiros ou quaisquer terceiros, desde que aprovados pela Diretoria Executiva responsável.

### Eventos de negócio

Qualquer colaborador do Grupo Inter somente poderá aceitar convites para participação em eventos patrocinados ou promovidos por fornecedores e parceiros quando houver a concreta possibilidade de estabelecimento de vínculo comercial. Convites advindos de órgãos governamentais e outros agentes públicos só poderão ser aceitos se tiverem caráter institucional e forem estendidos a outras empresas. Para o aceite de qualquer das duas situações, é necessária a validação formal da Diretoria Executiva responsável.

Da mesma forma, o Grupo Inter somente convidará fornecedores e parceiros para eventos auto patrocinados ou autopromovidos quando houver a concreta possibilidade de estabelecimento de vínculo comercial. Órgãos governamentais e outros agentes públicos somente poderão ser convidados se o evento for de caráter exclusivamente institucional. Antes da realização de qualquer desses convites, é necessária a validação formal da Diretoria Executiva responsável.

Fornecedores e parceiros não poderão realizar eventos, tais como churrascos, para as equipes das obras do Grupo Inter.

## 3. Princípios de Conduta

## Ambiente de trabalho

O Grupo Inter propicia e incentiva um ambiente de trabalho saudável, produtivo e que garanta a qualidade física e moral de todos os colaboradores, exigindo deles o comprometimento com o negócio, o protagonismo, a transparência nas relações e o melhoramento contínuo.

Desse modo, no desenvolvimento de nossas atividades, nos comprometemos a:

- . Cumprir o combinado;
- . Obedecer as regras e políticas internas e as leis vigentes;
- . Usar roupas e acessórios que condizem com o ambiente corporativo;
- . Respeitar as pessoas, independentemente de sua posição hierárquica, religião, convicção filosófica ou política, nacionalidade, cultura, posição social ou econômica, origem, sexo, raça, capacidade física, orientação sexual, sendo rechaçada qualquer prática e discriminação;
- . Atuar com compromisso com a qualidade, inovação e empreendedorismo coletivo;
- . Inibir e denunciar atitudes abusivas, quer seja através de palavras, gestos ou comportamentos contra a integridade física e moral de qualquer pessoa, que possam ser consideradas como assédio sexual ou moral.
- . Denunciar qualquer situação que viole o conteúdo deste Código e demais regras e políticas internas, bem como as leis vigentes.

## Qualidade, Segurança, Meio Ambiente e Saúde

Saúde e segurança são prioridades para o Grupo Inter. Todos aqueles que atuam em suas dependências devem respeitar e observar as normas e procedimentos de Saúde e Segurança do Trabalho.

Além disso, todos devemos dar o exemplo, orientar e fiscalizar o correto uso de Equipamentos de Proteção Individual e Coletivo, especialmente em canteiros de obra, bem como manter a limpeza, organização e segurança em todas as nossas instalações.

É expressamente proibido o consumo e/ou porte de bebidas alcoólicas ou qualquer tipo de droga, além da prática de jogos de azar, presenciais e virtuais, durante as atividades profissionais e no horário de trabalho.

O Grupo Inter apoia iniciativas de desenvolvimento sustentável alinhadas à legislação ambiental. Portanto, os colaboradores e terceiros devem conduzir suas atividades em total respeito ao meio ambiente, atentando-se para o uso de tecnologias e melhores práticas que conservem os recursos naturais e preservem o planeta.

É importante que todos estejam atentos aos aspectos e impactos ambientais, informando, imediatamente, às áreas de Segurança, Saúde e Meio Ambiente/SSMA e Jurídico, quaisquer

acidentes ambientais, bem como qualquer ato ou fato que possa vir a representar infração legal ou dano ambiental.

## Redes Sociais

O cuidado, proteção e zelo pela imagem do Grupo Inter é responsabilidade de todos.

Neste sentido, é permitido ao colaborador associar seu perfil pessoal ao nome e/ou marca de qualquer empresa do Grupo, com o objetivo de demonstrar o seu vínculo profissional, desde que o conteúdo não exponha negativamente a imagem da Companhia. Caso aconteça, a responsabilidade será unicamente do autor.

Contudo, toda e qualquer comunicação oficial do Grupo Inter somente será feita em suas redes oficiais, por equipe responsável e especializada no conteúdo.

## Conflito de Interesse

Caracteriza-se conflito de interesses sempre que um colaborador utiliza de sua influência ou sobreposição seus interesses particulares aos interesses do Grupo Inter, resultando em benefício próprio e/ou prejuízo a alguma empresa do Grupo. Estas situações são vetadas em todas as relações envolvendo colaboradores e/ou representantes da empresa.

São exemplos de conflito de interesses, mas que não se limitam a esses:

- . Exercício de atividades conflitantes com os interesses do Grupo Inter, dentro do ambiente e horário de trabalho;
- . Uso de informações do Grupo ou obtidas por meio do Grupo para uso particular ou para terceiros;
- . Contratação de agente público no exercício do cargo, ainda que indireta ou como consultor, salvo os casos em que lei autorize a contratação;
- . Omissão de informação de grau de parentesco ou vínculo familiar e/ou afetivo com algum colaborador do Grupo Inter;
- . Obtenção de vantagens, de qualquer natureza, direta ou indiretamente, advindas de fornecedores, prestadores de serviços, clientes ou qualquer outra pessoa ou entidade interessada em criar relações comerciais com as empresas do Grupo.

Qualquer situação que caracterize e sugira conflito de interesses deverá ser informada ao líder imediato, à área responsável pela governança, riscos e compliance ou denunciada por meio do Canal Confidencial.

## Recursos e Ativos

Todos somos responsáveis pela guarda, zelo e conservação dos recursos e ativos do Grupo Inter, os quais devem ser utilizados para fins estritamente profissionais, de forma controlada e consciente.

Os recursos e sistemas de Tecnologia da Informação são exclusivos para execução das atividades laborais, sendo proibida a utilização de softwares não autorizados ou homologados pelo Grupo Inter, em computadores ou redes e sistemas utilizados pela Companhia.

O respeito ao nome e marca Inter engloba o cumprimento das leis e diretrizes de propriedade intelectual. Dessa forma, não é admitido copiar, reproduzir, transmitir, distribuir ou utilizar documentos, arquivos, modelos, metodologias, fórmulas, pesquisas, projetos, projeções, análises e relatórios produzidos pelo Grupo Inter.

Todo colaborador ou terceiro que utilize os recursos e ativos (máquinas, equipamentos, celulares, veículos e demais materiais cedidos pela Companhia para realização de suas atividades) do Grupo é responsável pela preservação, sendo indevido e intransferível o uso para terceiros por meio de empréstimos, locações ou permutas. O Grupo Inter reserva-se o direito de monitorar a utilização de seus recursos e ativos.

É expressamente proibido dar carona a terceiros ou transportar objetos de terceiros nos veículos da frota Inter.

## Confidencialidade

Informação confidencial, estratégica ou privilegiada é aquela que, se mal utilizada, pode causar algum prejuízo à Companhia, como perdas financeiras ou danos irreparáveis à imagem.

São exemplos deste tipo de informação, mas não se limitando a estes: dados de colaboradores, clientes e fornecedores, registro de reuniões, preços, planos de aquisições, fusões ou incorporações, resultados do negócio ainda não divulgados, políticas e práticas de gestão dos negócios, desenvolvimento de novos produtos ou projetos e informações de empresas com as quais fazemos negócios.

Devemos manter o sigilo de todas as informações internas, protegendo-as de acessos e divulgações indevidas. Por isso, é proibido o transporte e cópia, física ou eletrônica, de qualquer informação do Grupo Inter, durante e após o término da relação de trabalho ou prestação de serviço, salvo autorização formal. Além disso, é imprescindível que assuntos relacionados a qualquer empresa do Grupo não sejam discutidos em público, utilizar senha individual para proteção de arquivos, não deixar documentos sigilosos à vista e destruí-los antes de descartar. Por fim, todos os colaboradores devem assinar e respeitar o Termo de Confidencialidade do Grupo Inter, que faz parte do contrato de trabalho.

O uso de informações confidenciais em benefício próprio ou de terceiros é crime e está sujeito a sanções trabalhistas e/ou penais.

## 4. Ações Institucionais

### Doações e Patrocínios

O Grupo Inter poderá conceder doações ou patrocínios com o intuito de cumprir sua responsabilidade social corporativa ou divulgar sua marca e estreitar a comunicação da empresa com seus clientes, fornecedores e sociedade, respectivamente. Porém, essas ações deverão ser realizadas com o mais elevado padrão de transparência, integridade e legalidade.

Para tanto, os contratos deverão conter a assinatura de, no mínimo, dois diretores executivos e chancela do Jurídico. Deverão conter também cláusulas anticorrupção e de ciência e vinculação ao Código de Ética e Conduta do Grupo Inter.

Além disso, são proibidos doações e patrocínios:

- . Com a finalidade de obter vantagem inadequada ou influenciar a ação de qualquer pessoa, seja agente público, fornecedor, terceiro, dentre outros;
- . Para entidades e organizações com reputação inidôneas e histórico de corrupção e lavagem de dinheiro;
- . Para entidades e organizações que sejam administradas, direta ou indiretamente, por pessoas politicamente expostas ou por agentes públicos, que tenham suas atividades relacionadas com o negócio do Grupo Inter;
- . Para entidades e organizações em que colaboradores do Grupo Inter ou seus parentes de primeiro grau possuam algum tipo de participação societária e/ou poder de gestão.

O Grupo Inter não realiza qualquer tipo de doação para político e/ou partidos políticos, campanhas políticas e/ou candidatos para cargo público.

É permitido que colaboradores participem de atividades políticas desde que sejam sempre em caráter pessoal, fora do expediente de trabalho e em observância às diretrizes do Código de Ética e Conduta.

### Corrupção e Lavagem de Dinheiro

Práticas de corrupção são repudiadas e não admitidas em qualquer negócio do Grupo Inter, sejam ativas ou passivas, através de atos ou omissões, por via da criação e/ou manutenção de situações de irregularidade, de favorecimento ou fraudulentas.

Da mesma forma, o Grupo Inter não tolera e não admite qualquer prática de lavagem de dinheiro, desvios de recursos ou bonificações injustificadas, feitas para ocultar ou legitimar recursos financeiros ilícitos.

Qualquer indício de ocorrência de corrupção e lavagem de dinheiro deverá ser denunciado ao líder imediato, à área de Compliance ou por meio do Canal Confidencial.

### Acurácia nos registros contábeis

Nossos registros contábeis devem ser elaborados em rigorosa consonância com os Princípios Fundamentais de Contabilidade e as Normas Brasileiras de Contabilidade vigentes, de forma que qualquer possibilidade de erro ou viés seja eliminada.

## 5. Relacionamento

### Clientes

É dever de todo colaborador do Grupo Inter tratar os clientes com cortesia, presteza e igualdade, diligenciando todas as suas demandas com eficiência e transparência, de forma que cumpramos com o que fora combinado.

Os questionamentos, críticas e sugestões dos clientes deverão ser direcionados aos canais oficiais do Relacionamento com Cliente, por meio do telefone 0800 449 1006 e e-mail [sac@interconstrutora.com.br](mailto:sac@interconstrutora.com.br), e deverão receber tratamento adequado. Os nossos erros, quando identificados, deverão ser sanados com soluções ágeis, definitivas e exemplares.

Qualquer atitude de desinteresse e desrespeito com os clientes deverá ser comunicada ao líder imediato, à área de Compliance ou por meio do Canal Confidencial.

Em respeito às regras da Lei Geral de Proteção de Dados, é expressamente vedada a divulgação de dados transmitidos pelos clientes sem autorização prévia e expressa, salvo quando permitido por lei.

A satisfação dos nossos clientes é de responsabilidade de todos os colaboradores do Grupo Inter.

### Fornecedores, prestadores de serviços e parceiros

Alicerçamos nossa relação com fornecedores, prestadores de serviços e parceiros em ética, integridade e transparência.

Assim, devemos garantir que a aquisição de bens e serviços somente ocorra segundo a melhor relação custo/benefício para a Companhia, considerando-se qualidade, prazo, preço, dentre outros.

O Grupo Inter somente contratará fornecedores, prestadores de serviços e parceiros por meio de processos que impossibilitem o favorecimento de interesses pessoais, de parentes, ou de terceiros que estejam em desacordo com interesses da Companhia, ou que impliquem em práticas ilícitas ou ilegais.

Fornecedores, prestadores de serviços e parceiros que não possuem reputação ilibada não devem ser contratados pela Companhia. Para tanto, seus históricos de existência poderão ser avaliados.

Cabe ao Grupo Inter comunicar e exigir dos fornecedores, prestadores de serviços e parceiros o conhecimento do conteúdo deste Código de Ética e Conduta, bem como exigir o cumprimento da legislação aplicável, destacando-se as leis anticorrupção brasileiras, em especial à Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e à Lei Anticorrupção, nº 12.846/13.

### Empreiteiros

Os empreiteiros possuem papel fundamental no nosso negócio, pois são eles que fornecem a mão de obra necessária para o desenvolvimento dos nossos projetos. Desse modo, é fundamental que a atuação deles esteja sempre de acordo com os valores, políticas e princípios do Grupo Inter.

Cabe ao Grupo Inter comunicar e exigir dos empreiteiros o conhecimento do conteúdo deste Código de Ética e Conduta, bem como exigir o cumprimento da legislação aplicável, destacando-se as leis anticorrupção brasileiras, em especial à Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e à Lei Anticorrupção, nº 12.846/13.

Adicionalmente, devemos:

- . Exigir dos empreiteiros o cumprimento da legislação trabalhista e previdenciária;
- . Tornar obrigatório que todos os seus empregados utilizem os EPIs (Equipamentos de Proteção Individual);
- . Avisá-los e acompanhá-los para que realizem ações de preservação do meio ambiente;
- . Obrigar o cumprimento de todas as cláusulas do Contrato de Prestação de Serviços firmado com o Grupo Inter;
- . Tornar obrigatório que paguem pontualmente os salários, encargos e benefícios de seus empregados;
- . Não aceitar que sejam divulgadas as condições de serviços prestados ao Grupo Inter;
- . Tornar obrigatória a comunicação tempestiva da existência de alojamento para acomodação de empregados;
- . Tornar obrigatório que as condições dos alojamentos e dos canteiros de obras sejam adequadas à saúde e ao bem-estar dos seus empregados.

## Investidores e acionistas

Os interesses e resguardo dos direitos dos nossos investidores e acionistas têm sido objeto de trabalho do Grupo Inter, propiciando que eles estejam sempre alinhados às melhores práticas de governança corporativa, às normas e regulamentos da Comissão de Valores Mobiliários (“CVM” e da B3 S.A. – Brasil, Bolsa, Balcão (“B3”) aplicáveis.

Para tanto, é nosso dever manter um bom relacionamento com todos os investidores e acionistas, independentemente da quantidade de ações por eles detida, bem como adotar práticas claras e éticas, possibilitando informações íntegras, confiáveis, transparentes e objetivas.

As transações envolvendo os acionistas e as empresas do Grupo Inter devem ser devidamente divulgadas no nosso site, de acordo com a nossa Política de Transação com Partes Relacionadas. Além disso, todas as informações institucionais, inclusive financeiras, deverão ser divulgadas ao mercado, nos termos das leis aplicáveis.

A responsabilidade pelo contato com nossos investidores e acionistas é da área de Relacionamento com Investidores. Qualquer solicitação feita diretamente aos colaboradores deverá ser imediatamente encaminhada à esta área, para que possa ser atendida adequadamente, por meio do e-mail [ri@interconstrutora.com.br](mailto:ri@interconstrutora.com.br).

Reforçamos aos nossos colaboradores a importância do cumprimento das normas estipuladas pela CVM. Desse modo, é proibido aproveitar de informações privilegiadas do Grupo Inter para benefício próprio ou a terceiros, direta ou indiretamente, decorrente da venda ou compra das ações. A utilização indevida dessas informações é ilegal e pode resultar em sanções administrativas, cíveis e criminais.

Da mesma forma, não admitimos que qualquer colaborador compartilhe informações, atos, eventos ou fatos relevantes aos quais tenha acesso, em razão da posição que ocupa, em desacordo com a nossa Política de Divulgação de Ato ou Fato Relevante.

Por fim, nenhum colaborador está autorizado a comprar ou vender as ações das empresas do Grupo Inter durante os períodos de vedação à negociação, previstos em nossa Política de Negociação de Valores Mobiliários.

## Setor Público

A nossa relação com o setor público é pautada, como todas as demais relações, em ética, integridade e transparência. Dessa forma, é inaceitável que sejam oferecidos e concedidos, direta ou indiretamente, qualquer tipo de incentivo a autoridades ou agentes públicos no exercício de suas funções, ou por meio de terceiros ou qualquer pessoa indicada, não previstos na legislação, com o objetivo de subornar ou receber tratamento especial.

O Grupo Inter reitera a atenção e cumprimento às leis anticorrupção brasileiras, em especial à Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e à Lei Anticorrupção, nº 12.846/13,

estando obrigados a cumpri-las integralmente e abster-nos de praticar qualquer atividade que constitua ou possa constituir violação a elas.

### Imobiliárias e profissionais associados

As imobiliárias e os profissionais associados [esclarecer melhor o cargo/papel desses profissionais associados no negócio] são o elo entre o Grupo Inter e os nossos clientes, por isso, devemos garantir que eles conduzam suas atividades com profissionalismo, prestando um atendimento de qualidade e protegendo a nossa marca.

Cabe ao Grupo Inter comunicar e exigir das imobiliárias e dos profissionais associados o cumprimento do conteúdo deste Código de Ética e Conduta, da legislação trabalhista, previdenciária, fiscal e demais.

### Sindicatos

O Grupo Inter prima por manter uma relação de respeito e cordialidade com as entidades sindicais e respeita a livre associação de seus colaboradores. Os acordos coletivos negociados com responsabilidade são cumpridos, considerando-se os interesses dos colaboradores e os da Companhia.

### Mídias

As solicitações da imprensa são atendidas de forma transparente, desde que autorizadas pela área de Relacionamento com Investidores. Sendo assim, qualquer pedido de entrevistas a órgãos de imprensa deverá ser aprovado previamente por esta área. Pedidos de divulgação de imagem do Grupo Inter também deverão ser aprovados pela área de Relacionamento com Investidores e consultados na área de Marketing, para o correto uso da marca.

### Concorrência

O Grupo Inter acredita que a livre concorrência, leal e transparente, contribui para o aperfeiçoamento do mercado.

Sendo assim, o compartilhamento de informações, exceto as estratégicas e confidenciais, é permitido, desde que com o propósito de alcançar objetivos comuns e as partes se comprometam em manter o acesso restrito a elas.

## 6. Termo de ciência e compromisso

Declaro que recebi, li e compreendi o Código de Ética e Conduta do Grupo Inter. Estou ciente e de pleno acordo com os critérios, orientações estabelecidas e sua relevância para mim e para as empresas do Grupo.

Comprometo-me a cumpri-lo integralmente sob pena de sofrer as medidas administrativas punitivas e medidas rescisórias do meu contrato de trabalho e legislação vigente, respectivamente.

EXISTE ALGUMA SITUAÇÃO QUE DEVA SER DECLARADA EM RELAÇÃO A CONFLITOS DE INTERESSES PARA INFORMAÇÃO E/OU VALIDAÇÃO DA ÁREA RESPONSÁVEL PELA GOVERNANÇA, RISCOS E COMPLIANCE?

Sim

---

---

Não

Nome Completo: \_\_\_\_\_

Área: \_\_\_\_\_

Assinatura: \_\_\_\_\_

Data: \_\_\_\_\_

# POLÍTICA ANTICORRUPÇÃO

---

GRUPO INTER



## Sumário

1. Introdução .....	2
2. Objetivo .....	2
3. Abrangência.....	2
4. Relação com outras Políticas Internas.....	2
5. Definições .....	3
6. Diretrizes .....	3
Relacionamento com Fornecedores, Parceiros e Prestadores de serviços .....	3
Relacionamento com o Poder Público .....	3
Recebimento de brindes e presentes .....	4
Pagamento de facilitações .....	4
Doações e patrocínios.....	4
7. Combate à Lavagem de Dinheiro .....	4
8. Prática de due diligence .....	5
9. Treinamento, Comunicação e dúvidas.....	5
10. Denúncias e não retaliação .....	5
11. Investigação.....	6
12. Medidas disciplinares.....	6
13. Medidas de controle interno.....	6
14. Termo de ciência e compromisso.....	7

## 1. Introdução

Reforçando o nosso compromisso em manter os mais corretos e adequados princípios e padrões de ética, integridade e governança corporativa, não tolerando nenhuma forma de corrupção, suborno ou qualquer outra prática que fira nossos valores, a Inter Construtora e Incorporadora S.A. (“**Companhia**”) adota a presente Política Anticorrupção, renovando, assim, o compromisso de cumprir rigorosamente todas as leis aplicáveis, incluindo as leis anticorrupção brasileiras, em especial a Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e a Lei Anticorrupção, nº 12.846/13, e outras normas relativas às relações com a Administração Pública.

Esta Política Anticorrupção (“**Política**”), aprovada pelo nosso Conselho de Administração Companhia em 31 de maio de 2021, contém diretrizes, padrões e procedimentos desenvolvidos para garantir que a Companhia, suas controladas e controladores (“**Grupo Inter**”) e todos aqueles que atuem em nosso nome entendam e ajam de acordo com as leis anticorrupção, aplicáveis a todas as relações com departamentos ou agências da Administração Pública, bem como com entes privados.

A violação das leis anticorrupção pode expor o Grupo Inter e seus colaboradores a graves consequências, incluindo penalidades administrativas, judiciais e criminais.

## 2. Objetivo

Esta Política orienta a atuação do Grupo Inter na prevenção e combate à corrupção e lavagem de dinheiro em seus negócios e faz parte do nosso Programa de Integridade.

## 3. Abrangência

Esta Política Anticorrupção se aplica a todos os colaboradores do Grupo Inter, incluindo membros do Conselho de Administração, Diretoria Executiva, colaboradores efetivos e estagiários. Aplicando-se ainda a terceiros, fornecedores e prestadores de serviços, que atuem em nome ou no interesse do Grupo Inter.

Todas as pessoas acima relacionadas deverão prestar compromisso de conhecimento, comprometendo-se ao fiel cumprimento das regras aqui estabelecidas.

A presente Política regula tanto a nossa relação com a Administração Pública, em todas as suas esferas, bem como serviços de natureza pública, também se aplicando às nossas relações com entidades privadas.

## 4. Relação com outras Políticas Internas

A presente Política Anticorrupção integra o Programa de Integridade do Grupo Inter e se relaciona com

todas as demais políticas e normas internas que fazem parte deste programa, complementando-as e sendo complementada por elas.

## 5. Definições

Código de Ética e Conduta – documento do Grupo Inter que reúne todas as regras a serem seguidas por todos seus colaboradores e terceiros, e que estabelece padrões de comportamento e formas de agir, de acordo com a missão, os valores e os objetivos da Companhia.

Conselho de Administração – Órgão colegiado e estatutário da Companhia, responsável pela supervisão das atividades de gestão do Grupo Inter e pelas orientações gerais dos negócios do Grupo.

*Due diligence* – A *due diligence* é um processo estruturado de pesquisa, auditoria, investigação e avaliação de riscos e oportunidades nas operações de negócios.

GRCP (Governança, Risco, Compliance e Privacidade) – área do Grupo Inter cujo objetivo, dentre outros, é assegurar a transparência dos processos de negócio, garantindo aderência às disposições das leis, políticas, normas, estatutos e outros regulamentos internos.

Serviços de natureza pública – serviços públicos, porém que não sejam prestados diretamente pela Administração Pública, mas sim por meio de delegação, como no caso das serventias extrajudiciais (cartórios).

## 6. Diretrizes

### 6.1. Relacionamento com Fornecedores, Parceiros e Prestadores de Serviços

O Código de Ética e Conduta do Grupo Inter estabelece que fornecedores, parceiros e prestadores de serviços que não possuem reputação ilibada não devem ser contratados pela Companhia. Para tanto, seus históricos de existência poderão ser avaliados.

Cabe ao Grupo Inter comunicar e exigir dos fornecedores, parceiros e prestadores de serviços o conhecimento do conteúdo desta Política Anticorrupção, do Código de Ética e Conduta, bem como exigir o cumprimento da legislação aplicável, destacando-se as leis anticorrupção brasileiras, em especial a Lei de Prevenção à Lavagem de Dinheiro, nº 9.613/98, e a Lei Anticorrupção, nº 12.846/13.

### 6.2. Relacionamento com o Poder Público

O Grupo Inter reforça o seu compromisso no combate à corrupção e proíbe qualquer ato desta natureza, seja de forma direta ou indireta, perante Agentes Públicos ou que venham a exercer qualquer função pública nas três esferas da Federação ou em qualquer órgão público, seja nacional ou

estrangeiro.

Qualquer colaborador, prestador de serviço, fornecedor ou parceiro, que em razão de suas funções atuem em nome do Grupo Inter, está proibido de oferecer qualquer tipo de vantagem indevida, não importando sua natureza, para agente público no intuito de obter qualquer tipo de facilitação que favoreça o Grupo Inter ou a si próprio.

### 6.3. Recebimento de brindes e presentes

Como previsto em nosso Código de Ética e Conduta, o recebimento e a oferta de brindes e presentes não podem ser utilizados como forma de influenciar qualquer decisão de negócio.

O recebimento somente poderá acontecer com a finalidade de atender às funções de lembrança da marca e/ou agradecimento. Ainda assim, deverão ser institucionais, tais como materiais de escritório e souvenirs, e sem valor de mercado.

No caso de recebimento de brindes e presentes diferentes dos supracitados, só poderão ser aceitos se declarados à Comunicação Interna (RH) para realização de sorteio entre os colaboradores ou para serem destinados a premiações internas. Quaisquer outros tipos de benefícios ou vantagens, incluindo viagens e hospedagens, deverão ser recusados. Especificamente almoços e jantares poderão ser aceitos, desde que não sejam recorrentes.

Da mesma forma, nós somente podemos ofertar brindes e presentes institucionais, desenvolvidos como parte da estratégia de comunicação do Grupo Inter, a clientes, fornecedores, parceiros ou quaisquer terceiros, desde que aprovados pela Diretoria Executiva responsável.

### 6.4. Pagamento de facilitações

O Grupo Inter repudia e proíbe o pagamento ou oferta de facilitações por seus colaboradores, fornecedores ou parceiros de negócios.

Pagamento de facilitação se refere usualmente à oferta de valores em dinheiro ou benefícios pessoais para agente público no intuito de acelerar processos.

### 6.5. Doações e patrocínios

O Código de Ética e Conduta do Grupo Inter prevê as regras que regem a possibilidade de concessão de doações e/ou patrocínios, sendo expressamente vedado qualquer tipo de doação para político e/ou partidos políticos, campanhas políticas e/ou candidatos para cargo público.

## 7. Combate à Lavagem de Dinheiro

A prática de lavagem de dinheiro é classificada como crime, conforme previsto na Lei n. 9.613/98, e o

Grupo Inter repudia qualquer prática desta natureza. Por este motivo possui medidas de controle que visam impedir este tipo de prática.

Caso identifique indícios de lavagem de dinheiro, os órgãos competentes serão acionados e os envolvidos punidos na forma da lei.

## 8. Prática de *due diligence*

O Grupo Inter faz uso de práticas de *due diligence* na escolha de contratação de fornecedores, parceiros de negócios e aquisição de terrenos, sempre no intuito de evitar que o Grupo Inter estabeleça relações negociais com entidades e pessoas envolvidas em atos de corrupção e/ou de lavagem de dinheiro, preservando assim nossos valores éticos e morais.

## 9. Treinamento, Comunicação e dúvidas

Além da assinatura do Termo de Ciência e Compromisso, no momento da admissão, o conteúdo desta Política Anticorrupção será levado ao conhecimento de todos os colaboradores do Grupo Inter por meio de treinamentos periódicos e materiais informativos.

## 10. Denúncias e não retaliação

Todos aqueles abrangidos por esta Política Anticorrupção deverão relatar qualquer ato ou indício que a viole, bem como infrações ou desconformidades com as políticas, procedimentos e regulamentos internos do Grupo Inter e da legislação vigente, assegurando a proteção dos padrões éticos adotados pelo Grupo e preservando sua imagem no mercado.

Qualquer pessoa que não se sinta confortável e segura para relatar algum fato que esteja lhe causando incômodo ou desconfiança, poderá optar por realizar uma denúncia, identificada ou anônima, por meio do nosso Canal Confidencial.

Site: <https://interconstrutora.legaletica.com.br/>

Telefone: 0800 400 3333

E-mail: [interconstrutora@legaletica.com.br](mailto:interconstrutora@legaletica.com.br)

Nosso Canal Confidencial é operado por uma empresa terceirizada especializada no recebimento de denúncias de forma confidencial e com preservação do anonimato. Embora não seja necessária a identificação do denunciante, é fundamental agir com responsabilidade ao efetuar um relato, que deve ser consistente e verídico.

O anonimato é garantido e o Grupo Inter não admite qualquer forma de retaliação, discriminação ou

sanção contra qualquer indivíduo que exponha uma preocupação verdadeira e de boa fé. Além disso, a Companhia se compromete à ampla proteção contra retaliações àqueles que decidirem utilizar o canal confidencial.

## 11. Investigação

As denúncias recebidas serão submetidas a processo interno de investigação para averiguação dos fatos e seus autores. Se após o processo de investigação ficar comprovado a prática de ato que viole esta política, serão aplicadas as devidas medidas disciplinares mencionadas no item 12 desta Política, observando-se o grau de gravidade do ato praticado, a lei aplicável ao caso e as circunstâncias do fato.

## 12. Medidas disciplinares

Toda denúncia será objeto de investigação imediata, guiada por processos íntegros, éticos e seguros.

Após o processo de investigação, caso seja constatada a prática de qualquer ato que transgrida esta Política ou a legislação aplicável, medidas corretivas serão imediatamente adotadas e aplicadas de maneira exemplar, sempre de acordo com as circunstâncias, gravidade e a lei de referência.

Qualquer das partes que viole o disposto nesta Política estará sujeita às sanções disciplinares listadas abaixo:

- Advertência oral;
- Advertência por escrito;
- Suspensão de contrato;
- Demissão sem justa causa;
- Demissão por justa causa;
- Exclusão do fornecedor, parceiro ou agente intermediário do Grupo Inter;
- Ação judicial cabível.

## 13. Medidas de controle interno

As medidas de controle interno visam o monitoramento de atividades que ofertem algum tipo de risco de conformidade, identificando eventuais falhas no atendimento de requisitos normativos internos ou externos.

O Grupo Inter monitorará as operações por meio de:

- i. Avaliação dos cadastros de clientes e parceiros de negócios;
- ii. Revisões periódicas das políticas internas, levando em consideração alterações nas legislações aplicáveis, bem como boas práticas de governança;

- iii. Política de portas abertas, facilitando o diálogo com todas as áreas do Grupo;
- iv. Treinamentos e ações internas com o objetivo de ampliar o conhecimento do conteúdo desta Política e demais; e
- v. Implementação de uma estrutura de controles internos.

As ações de monitoramento serão executadas continuamente, a fim de garantir a conformidade nos processos de negócio.

Todos os colaboradores do Grupo Inter se comprometem com o devido respeito à esta Política, ao Código de Ética e Conduta, e outras normas internas, bem como Leis, Decretos e Regulamentos que já existam ou que venham a existir, que versem sobre o combate à corrupção e à lavagem de dinheiro, estando por isso sujeitos ao monitoramento constante em suas ações.

O previsto no item acima também se aplica a todas as operações, propostas e negócios, celebrados pelo Grupo Inter.

O Grupo Inter se compromete a implementar as melhores medidas de controle e, também, a revisá-las periodicamente.

## 14. Termo de ciência e compromisso

Declaro que recebi, li e compreendi a Política Anticorrupção do Grupo Inter. Estou ciente e de pleno acordo com os critérios, orientações estabelecidas e sua relevância para mim e para as empresas do Grupo.

Comprometo-me a cumpri-lo integralmente sob pena de sofrer as medidas administrativas punitivas e medidas rescisórias do meu contrato de trabalho e legislação vigente, respectivamente.

Nome Completo: \_\_\_\_\_

Área: \_\_\_\_\_

Assinatura: \_\_\_\_\_

Data: \_\_\_\_\_

# POLÍTICA DE TRANSAÇÕES COM PARTES RELACIONADAS

---

GRUPO INTER

## Sumário

1.	Objetivo .....	3
2.	Abrangência.....	3
3.	Definições .....	4
4.	Procedimento .....	6
4.1	Análise Prévia .....	6
4.2	Aprovações.....	7
5.	Penalidades .....	9
6.	Obrigaç�o de divulga�o .....	9
7.	Disposi�es finais .....	9

## 1. Objetivo

**1.1.** A presente Política de Transações com Partes Relacionadas (“**Política**”), aprovada em reunião do Conselho de Administração da Inter Construtora S.A. (“**Companhia**”), realizada em 31 de maio de 2021, tem como objetivo definir regras, no âmbito de todas as relações da Companhia, suas controladas e controladores (“**Grupo Inter**”), com colaboradores, gestores, gerentes, diretores, fornecedores, concorrentes e diversas outras pessoas ou empresas que possuam relações ou interesses com alguma entidade da Companhia, para assegurar que todas as operações e tomadas de decisão sejam administradas e direcionadas visando exclusivamente aos interesses da Companhia, de seus acionistas, especialmente no que tange ao envolvimento de partes relacionadas e conflito de interesses, bem como quaisquer situações com risco potencial nesses sentidos, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, conforme alterada (“**Lei das Sociedades por Ações**”) e demais leis e regulamentação de mercado de capitais aplicáveis, e das boas práticas de governança corporativa.

**1.2.** O simples fato da existência de relacionamentos com Partes Relacionadas (conforme definido abaixo) pode significar comprometimento nas transações da Companhia com outras partes requerendo, desta forma, que: (i) a existência de relacionamentos com Partes Relacionadas seja divulgada adequadamente; (ii) as decisões relativas às operações e tomadas de decisão sejam feitas evitando-se uma influência direta de Partes Relacionadas (conforme definido abaixo); e (iii) as transações desta natureza sejam realizadas respeitando termos e condições habituais de mercado, conforme descrito no item 5 abaixo.

## 2. Abrangência

**2.1** A presente Política abrange, mas não se limita a, todos os administradores da Companhia e de suas controladas, diretas ou indiretas, bem como aos seus respectivos procuradores, responsáveis técnicos e/ou administrativos, empregados, colaboradores, consultores, terceiros interpostos e seus respectivos familiares, incluindo cônjuges ou companheiros(as), seus filhos, os filhos de seus cônjuges ou companheiros(as), e seus dependentes ou os de seus cônjuges e companheiros(as).

**2.2** É devida e esperada a lealdade de todas as pessoas descritas no *caput* acima em relação às suas decisões, transações e operações, sendo exigido que os interesses da Companhia sempre se sobreponham aos interesses particulares dos tomadores de decisão.

**2.3** É obrigação de todos (i) guardar sigilo e confidencialidade das informações relativas a atos ou fatos relevantes às quais tenham acesso privilegiado em razão do cargo ou posição que ocupam, até a

sua divulgação ao mercado, (ii) zelar para que subordinados e terceiros de sua confiança também o façam, respondendo solidariamente com estes na hipótese de descumprimento, bem como (iii) jamais usar as informações às quais tenha acesso para realizar negócios particulares ou beneficiar terceiros, independente do resultado.

### 3. Definições

**3.1.** Nos termos da regulamentação aplicável, em especial o Pronunciamento Técnico CPC nº 5 (“**CPC 5**”) emitido pelo Comitê de Pronunciamentos Contábeis – CPC e aprovado pela Comissão de Valores Mobiliários por meio da Deliberação da CVM nº 642, de 7 de outubro de 2010 (“**Deliberação 642**”), é considerada parte relacionada, para fins da presente Política, a pessoa ou a sociedade que está relacionada com a Companhia conforme indicado a seguir (“**Parte Relacionada**”):

- (i) uma pessoa ou um membro próximo de sua família, que:
  - (a) tiver o controle pleno ou compartilhado da Companhia;
  - (b) tiver Influência Significativa (conforme definido abaixo) sobre a Companhia; ou
  - (c) for membro do pessoal chave da administração da Companhia ou de sua controlada.
  
- (ii) uma sociedade que:
  - (a) pertença ao mesmo grupo econômico da Companhia;
  - (b) seja controladora, controlada ou coligada da Companhia;
  - (c) estiver, junto com a Companhia, sob controle conjunto (*joint venture*) de uma terceira sociedade;
  - (d) estiver sob controle conjunto (*joint venture*) de uma terceira sociedade e a Companhia for coligada dessa terceira sociedade;
  - (e) seja controlada, de modo pleno ou sob controle conjunto, por uma pessoa identificada no item (i) acima;
  - (f) esteja sob Influência Significativa de qualquer pessoa identificada na letra (i)(a) acima, ou se esta pessoa for membro do pessoal chave da administração da sociedade (ou de controladora da sociedade).

**3.1.1.** Para os fins do item 3.1 acima, “**Influência Significativa**” é o poder de participar nas decisões financeiras e operacionais de uma entidade, mas que não caracterize o controle sobre essas políticas. Influência Significativa pode ser obtida por meio de participação societária, disposições estatutárias ou acordo de acionistas.

**3.1.2.** Para os fins do item 3.1(i) acima, serão considerados membros próximos da família de uma pessoa aqueles membros da família dos quais se pode esperar que exerçam influência ou sejam influenciados pela pessoa nos negócios desses membros com a Companhia e incluem:

**3.1.2.1.** os filhos da pessoa, cônjuge ou companheiro(a);

**3.1.2.2.** os filhos do cônjuge da pessoa ou de companheiro(a); ou

**3.1.2.3.** dependentes da pessoa, de seu cônjuge ou companheiro(a).

**3.2.** Para os fins do item 3.1 acima, pessoal chave da administração são as pessoas que têm autoridade e responsabilidade pelo planejamento, direção e controle das atividades da Companhia, direta ou indiretamente, incluindo qualquer administrador (executivo ou outro) da Companhia.

**3.3.** Ao considerar cada um dos possíveis relacionamentos com Partes Relacionadas, a atenção deve ser direcionada para a essência do relacionamento e não meramente para sua forma legal. Nesse sentido, no contexto desta Política, não são consideradas Partes Relacionadas:

**3.3.1.** duas sociedades simplesmente por terem administrador ou outro membro do pessoal chave da administração em comum, ou porque um membro chave da administração da sociedade exerce Influência Significativa sobre a outra sociedade;

**3.3.2.** dois investidores simplesmente por compartilharem o controle conjunto sobre um empreendimento controlado em conjunto (*joint venture*);

**3.3.3.** (a) entidades que proporcionam financiamentos; (b) sindicatos; (c) entidades prestadoras de serviços públicos; e (d) departamentos e agências governamentais que não controlam, de modo pleno ou em conjunto, ou exercem Influência Significativa sobre a Companhia, simplesmente em virtude dos seus negócios normais com a Companhia (mesmo que possam afetar a liberdade de ação da Companhia ou participar no seu processo de tomada de decisões);  
e

**3.3.4.** cliente, fornecedor, franqueador, concessionário, distribuidor ou agente geral com quem a Companhia mantém volume significativo de negócios, meramente em razão da resultante dependência econômica.

**3.4.** É considerada transação com Parte Relacionada, para fins desta Política e nos termos da legislação aplicável, qualquer operação da Companhia que trate de transferência de bens, recursos, direitos, obrigações, contratação ou prestação de serviços, negócios, disputas ou ações que envolvam Partes Relacionadas, independentemente de haver ou não um preço em contrapartida à transação e

de estarem representadas por outras pessoas jurídicas ou físicas (“**Transações com Partes Relacionadas**”).

**3.4.1.** A definição se estende a situações em que uma pessoa que tem, direta ou indiretamente, por meio de um familiar ou uma pessoa com quem convive, com quem é associado ou com quem tenha relacionamento próximo e íntimo, um interesse pessoal suficientemente relevante para aparentar influenciar ou gerar restrição no exercício objetivo e isento de suas atribuições na Companhia.

**3.4.2.** Os interesses também podem ser pessoais, científicos, assistenciais, educacionais, curriculares, religiosos, sociais e econômicos, podendo ocorrer de forma direta ou indireta, cometido por ação ou omissão.

**3.4.3.** As definições contidas na presente Política são meramente exemplificativas.

**3.4.4.** Para quaisquer definições, análises ou julgamento de operações de quaisquer pessoas físicas ou jurídicas pertencentes, sob qualquer vínculo, à Companhia, além de todo o arcabouço legal aplicável, deve-se considerar também:

- o Estatuto Social da Companhia;
- o Código de Conduta da Companhia;
- as políticas internas e procedimentos relacionados à contratação ou estabelecimento de parcerias que envolvam, entre outros, os negócios da Companhia; e
- a Lei das Sociedades por Ações.

## 4. Procedimento

### 4.1. Análise Prévia

**4.1.1.** Anualmente, a Companhia solicitará o preenchimento de uma declaração de conflito de interesses ou existência de relacionamento com Partes Relacionadas (“**Declaração**”) das pessoas que se enquadram na presente Política, bem como para outras que entender pertinente no âmbito da sua competência, por meio de um questionário que deverá ser (i) firmado pelo declarante e seu superior imediato, (ii) recebido e analisado por um Comitê Transitório, que será formado por um representante do Conselho de Administração, um representante da Diretoria Executiva, um representante da área de Governança, Riscos, Compliance e Privacidade e um representante do Jurídico, sendo vedada a participação de membros conflitados, a serem indicados, sob demanda, pelo Diretor Presidente ou, na ausência ou impedimento dele, pelo Diretor Vice-Presidente ou, na ausência ou impedimento de ambos, pelo Conselho de Administração da Companhia, com a abstenção de voto dos membros

impedidos, conforme aplicável, e (iii) colocado à disposição do Conselho de Administração, dependendo dos achados, assuntos, posição dos envolvidos e impedimentos.

**4.1.2.** Independente da periodicidade do fornecimento da Declaração, é obrigação do administrador ou pessoa envolvida em qualquer operação ou transação da Companhia, comunicar o eventual conflito de interesse ou existência de relacionamento com Partes Relacionadas, a sua natureza e extensão, de forma completa e a qualquer tempo, não devendo estar restrito à iniciativa da Companhia.

**4.1.3.** Não obstante, qualquer pessoa, ainda que estranha a Transação com Partes Relacionadas, poderá declarar atos ou fatos que entenda configurarem conflitos de interesses ou envolvam Partes Relacionadas, devendo se reportar ao Diretor Presidente, quando este não for parte relacionada do assunto, ou pelo Diretor Vice Presidente, quando este não for parte relacionada do assunto ou pelo Diretor Financeiro, quando este não for parte relacionada ao assunto, nessa ordem ou a qualquer outro canal de denúncias ou comunicação da Companhia.

**4.1.4.** Em caso de configuração de conflito de interesses, o(a) envolvido(a) deve se afastar, imediatamente, do processo específico, opinião e da tomada de decisão respectiva ao seu conflito, devendo aguardar orientações superiores e o cumprimento do processo de análise previsto na presente Política, mas em nenhuma hipótese o envolvido deve deixar de cumprir seus deveres legais e de proteção aos demais riscos da Companhia.

## 4.2. Aprovações

**4.2.1.** Os casos relacionados a conflitos de interesses ou Transações com Partes Relacionadas devem ser previamente comunicados ao Comitê Transitório, bem como constados em ata (descrevendo o interesse envolvido, extensão, natureza e detalhamento), sendo que:

**4.2.1.1.** os casos que o Comitê Transitório entender não serem relevantes em razão da matéria, valor envolvido ou situação, serão tomadas as decisões após ouvido o Diretor Presidente, quando este não for parte relacionada do assunto, ou o Diretor Vice-Presidente, quando este não for parte relacionada do assunto ou o Diretor Financeiro, quando este não for parte relacionada do assunto, nessa ordem, e o assunto deverá ser reportado ao Conselho de Administração por meio de relatórios trimestrais;

**4.2.1.2.** os casos que o Comitê Transitório entender serem relevantes em razão da matéria, valor envolvido ou situação, deverão ser reportados de forma imediata e formal ao Conselho de Administração, para emissão de decisão;

- 4.2.2.** O Comitê Transitório atuará de forma a garantir que as Transações com Partes Relacionadas:
- 4.2.2.1.** sejam realizadas por escrito, especificando-se as suas principais características, inclusive acerca da possibilidade de rescisão, pela Companhia, de qualquer Transação com Parte Relacionada que seja de trato sucessivo, em condições equivalentes às aquelas disponíveis nos contratos com partes não relacionadas;
  - 4.2.2.2.** sejam realizadas a preços, prazos e taxas usuais de mercado ou de negociações anteriores que representem condições comutativas; e
  - 4.2.2.3.** estejam claramente refletidas nas demonstrações financeiras.
- 4.2.3.** O Conselho de Administração, a seu critério, terá acesso a todos os documentos relacionados às Transações com Partes Relacionadas, incluindo quaisquer pareceres ou opiniões técnicas que a instância apropriada tenha recebido e a própria análise por ela realizada.
- 4.2.4.** Uma vez realizada a identificação e avaliação pelo Comitê Transitório das Transações com Partes Relacionadas, caberá ao Conselho de Administração da Companhia apreciar e aprovar, nos Termos do Estatuto Social. Na hipótese de a transação não superar os limites previstos no Estatuto Social, a competência para aprovar a operação é do Comitê Transitório.
- 4.2.5.** A Companhia, por meio de sua administração, deverá envidar todos os esforços necessários para dar maior transparência aos termos e condições das Transações com Partes Relacionadas.
- 4.2.6.** Caso a operação seja autorizada, sem prejuízo das demais regras estabelecidas nesta Política, as seguintes diretrizes deverão ser observadas:
- 4.2.6.1.** transparência (requer que, de acordo com a relevância, as informações sejam refletidas nos relatórios institucionais, , reporte adequado das condições acordadas com a devida aplicação, bem como reflexos destas nas demonstrações financeiras da Companhia);
  - 4.2.6.2.** competitividade (em termos de prazos, garantias, taxas, formas, preços e condições dos serviços ou produtos);
  - 4.2.6.3.** conformidade (o processo deve respeitar todo o processo de tomada de preço, verificação de condições técnicas e financeiras, coerência e aderência dos serviços prestados ou produtos fornecidos, responsabilidades e obrigações tratadas, controles adequados de segurança das informações, dentre outros); e

**4.2.6.4.** equidade (as negociações devem ocorrer entre partes independentes, com formas e procedimentos que impeçam discriminação, privilégios ou oportunidades de negócio em benefício individual ou de terceiros).

## 5. Penalidades

**5.1.** Qualquer violação ao disposto na presente Política pode configurar falta grave em relação ao vínculo ou relação que quaisquer de seus membros tenha com a Companhia, além de poder configurar ato ilícito civil e/ou criminal.

**5.2.** No exercício dos seus direitos, e de acordo com a legislação, a Companhia procederá a identificação e processamento da apuração, podendo concluir pela punição administrativa (*enforcement*) dos membros que violarem quaisquer aspectos da presente Política.

**5.3.** Ademais, a divulgação de qualquer informação importante e/ou reservada da Companhia que não seja pública, com prática de atos ou fatos que busquem a intenção de vantagem própria ou mesmo que revele a terceiros, independente do resultado, bem como a prática de *insider trading* configura ato ilícito, pelo comportamento desleal que viola a segurança, concorrência leal, a competitividade e igualdade de condição jurídica no mercado. Além de consequências no âmbito cível e administrativo, as penalidades previstas no ordenamento jurídico brasileiro chegam a ser privativas de liberdade (reclusão) e multa de até 3 (três) vezes o montante da vantagem ilícita obtida em decorrência do crime.

## 6. Obrigação de Divulgação

**6.1.** A Companhia está obrigada a divulgar Transações com Partes Relacionadas, em conformidade com o artigo 247 da Lei das Sociedades por Ações, com a Instrução da CVM nº 480, de 7 de dezembro de 2009, conforme alterada (“**Instrução CVM 480**”) e com a Deliberação 642.

**6.2.** A Companhia deve divulgar informações sobre Transações com Partes Relacionadas por meio de suas demonstrações contábeis periódicas, do Formulário de Referência da Companhia ou, ainda, quando a operação configurar fato relevante, nos termos da legislação aplicável, de modo a assegurar a transparência do processo aos acionistas, aos investidores e ao mercado.

## 7. Disposições Finais

**7.1.** A presente Política deverá ser revisitada constantemente, quer seja para assegurar a melhoria contínua das práticas de governança corporativa, quer seja em razão de alterações estatutárias,

legislativas ou demais normatizações, devendo ser revisada, aprovada e registrada em ata do Conselho de Administração da Companhia.

**7.2.** A presente Política entra em vigor na data de sua aprovação pelo Conselho de Administração da Companhia e vigerá por prazo indeterminado, ou até que haja deliberação pelo Conselho de Administração da Companhia em sentido contrário.

**7.3.** Esta Política poderá ser consultada no site de Relações com Investidores da Companhia ([www.ri.interconstrutora.com.br](http://www.ri.interconstrutora.com.br)).

\* \* \*

# Política de Resposta a Incidentes de Segurança da Informação

---

GRUPO INTER



## Sumário

<b>Glossário</b> .....	2
<b>1. Introdução</b> .....	3
<b>2. Objetivo</b> .....	3
<b>3. Abrangência</b> .....	3
<b>4. Definições e Tipos de incidentes</b> .....	3
<b>5. Relatando a ocorrência de um incidente de segurança</b> .....	4
<b>6. Contenção e recuperação</b> .....	5
<b>7. Investigação e análise de risco</b> .....	5
<b>8. Notificação</b> .....	6
<b>9. Avaliação e resposta</b> .....	7
<b>10. Violação e penalidades</b> .....	7
<b>11. Revisão desta Política</b> .....	8
<b>ANEXO 01</b> .....	9

## Glossário

- a) Ativo de informação – informações essenciais para os negócios da empresa passíveis de valoração.
- b) Confidencialidade da informação – quando a informação não está disponível ou revelada a quem não tenha autorização para acessá-la.
- c) Dados pessoais – são informações vinculadas à uma pessoa natural e que podem identificá-la de alguma forma, como por exemplo o nome, número de CPF ou RG, endereço etc.
- d) Disponibilidade da informação – quando a informação está acessível e utilizável quando solicitada por alguém que tenha autorização para acessá-la.
- e) Evento de segurança da informação – Trata-se de uma ocorrência identificada de um estado de sistema, serviço ou rede, que indique a possibilidade de violação da Política de Segurança da Informação ou uma falha de controles, ou ainda uma situação desconhecida, que seja relevante para a segurança da informação.
- f) Segurança da informação – quando são implementadas ações que visam proteger a confidencialidade, integridade e disponibilidade da informação. Estas ações também podem visar a preservação da autenticidade, responsabilidade, não repúdio e confiabilidade.
- g) Tratamento de dados pessoais – qualquer operação realizada com dados pessoais. Tais como coleta, recepção, transmissão, acesso, reprodução, armazenamento, arquivamento, entre outras.

## 1. Introdução

A Inter Construtora e Incorporadora S.A. (“**Companhia**”) coleta, mantém, processa e compartilha dados e informações, ativos valiosos que precisam ser devidamente protegidos.

Todo cuidado é tomado para proteger os dados pessoais de incidentes (seja acidental ou deliberadamente), a fim de evitar uma violação da proteção de dados que possa comprometer a segurança.

O comprometimento de informações, ferindo os princípios da confidencialidade, integridade ou disponibilidade, pode resultar em danos para as pessoas, dano à reputação, efeito prejudicial na prestação de serviços, não conformidade legislativa e/ou custos financeiros.

## 2. Objetivo

Esta Política de Resposta a Incidentes de Segurança da Informação (“**Política**”) estabelece o procedimento a ser seguido para garantir uma abordagem consistente e eficaz para gerenciamento de violação de dados e incidentes de segurança da informação em toda a Companhia.

O objetivo desta Política é conter quaisquer possibilidades de violações, para minimizar os riscos associados e considerar quais ações são necessárias para proteger os ativos de informação e evitar novas violações.

## 3. Abrangência

Esta Política se refere a todos os ativos de informação, incluindo os dados pessoais, mantidos pela Companhia independentemente do formato.

Esta Política se aplica a todos os empregados da Companhia, incluindo também prestadores de serviço, consultores, fornecedores e operadores de dados trabalhando para, ou em nome da Companhia (“**Colaboradores**”).

## 4. Definições e Tipos de incidentes

Para os fins desta Política, as violações de segurança da informação incluem as que já foram confirmadas e as suspeitas de incidentes.

Um incidente no contexto desta Política é um evento ou ação que pode comprometer a confidencialidade, integridade ou disponibilidade de sistemas ou dados, seja acidental ou deliberadamente, e que tenha causado, ou tem potencial para causar, danos aos ativos de informação da Companhia e/ou à sua reputação.

Um incidente inclui, mas não está restrito a:

- a) perda ou roubo de dados confidenciais ou sensíveis ou equipamento no qual tais dados são armazenados (por exemplo, perda de *laptop*, *pendrive*, *tablet* ou registro de papel);
- b) roubo ou falha do equipamento;
- c) falha do sistema;
- d) uso não autorizado, acesso ou modificação de dados ou sistemas de informação;
- e) tentativas (malsucedidas ou bem-sucedidas) de obter acesso não autorizado a informações ou sistema(s) de TI;
- f) divulgação não autorizada de informações sensíveis/confidenciais;
- g) desfiguração do site;
- h) ataque de invasores não autorizados;
- i) circunstâncias imprevistas, como incêndio ou inundação;
- j) erro humano;
- k) “falsa denúncia” onde a informação é obtida enganando a organização que detém isto.

## **5. Relatando a ocorrência de um incidente de segurança**

Qualquer indivíduo que acessa, usa ou gerencia as informações da Companhia é responsável por reportar violação de dados e incidentes de segurança da informação imediatamente para ao Gestor de TI (em [segurancadainformacao@interconstrutora.com.br](mailto:segurancadainformacao@interconstrutora.com.br)) e ao Encarregado de Tratamento de Dados Pessoais (DPO) em [privacidade@interconstrutora.com.br](mailto:privacidade@interconstrutora.com.br).

Se a violação ocorrer ou for descoberta fora do horário normal de trabalho, deve ser relatada assim que for possível.

No caso de incidente em razão de furto ou roubo de equipamento de propriedade da Companhia a autoridade policial deverá ser comunicada imediatamente e a cópia do boletim de ocorrência deverá ser apresentada ao Gestor de TI.

O relatório deve incluir detalhes completos e precisos do incidente, quando a violação ocorreu (datas e horários), quem está relatando, se os dados se referem a uma pessoa natural, a natureza das informações, descrição do problema, quais os efeitos e como foi descoberto. O Formulário de Relatório de Incidente deve ser preenchido como parte do processo de relato (modelo Anexo 1), e há uma versão no formato eletrônico na Intranet.

Todos os Colaboradores devem estar cientes de que qualquer violação da legislação de proteção de dados pode resultar na instalação de procedimento disciplinar.

## 6. Contenção e recuperação

O Encarregado de Tratamento de Dados Pessoais (“**DPO**”) determinará, em primeiro lugar, se a violação ofende dados pessoais, e o Gestor de TI, identificará se a violação ainda está ocorrendo. Se sim, medidas apropriadas serão tomadas imediatamente para minimizar o efeito da violação.

Quando se tratar de incidente de segurança da informação que afete dados pessoais, uma avaliação inicial será feita pelo DPO em conjunto com a pessoa responsável pela Segurança da Informação (“**SI**”), a fim de estabelecer a gravidade da violação, e com quem assumirá a liderança na investigação da violação, como o responsável pela investigação oficial.

O Chefe de Investigação (“**LIO**”, *Lead Investigation Officer*) estabelecerá se há algo que pode ser feito para recuperar quaisquer perdas e limitar os danos que a violação poderia causar.

O LIO estabelecerá quem pode precisar ser notificado como parte da contenção inicial e informará a polícia, quando apropriado.

Pode ser solicitado o aconselhamento de especialistas em qualquer setor da Companhia para resolver o incidente prontamente.

O LIO, em contato com a pessoa responsável pela SI, determinará o curso de ação adequado a ser tomado para garantir a resolução do incidente.

## 7. Investigação e análise de risco

Uma investigação será realizada pelo LIO imediatamente e sempre que possível, dentro de 24 horas da violação ser descoberta ou relatada.

O LIO investigará a violação e avaliará os riscos associados a ela, por exemplo, as potenciais consequências adversas para as pessoas, quão graves ou substanciais são e quão prováveis são de ocorrer.

A investigação deverá levar em consideração o seguinte:

- a) o tipo de dados envolvidos;
- b) sua sensibilidade;
- c) se as proteções estão ativadas (por exemplo, criptografias);
- d) o que aconteceu com os dados (por exemplo, foram perdidos ou roubados);
- e) se é possível fazer algum uso ilegal ou impróprio dos dados;

- f) os titulares de dados pessoais afetados pela violação, número de pessoas envolvidas e o potencial efeito sobre o(s) titular(es) dos dados;
- g) se existem consequências mais amplas para a violação.

## 8. Notificação

O LIO e/ou o DPO, estabelecerá se a Autoridade Nacional de Proteção de Dados (“ANPD”), o Ministério Público ou outro ente interessado, terá de ser notificado da violação e, em caso afirmativo, o mesmo deverá ser notificado dentro de 72 horas após tomar conhecimento da violação, quando viável.

Cada incidente será avaliado caso a caso, no entanto, o seguinte deverá ser considerado:

- a) se a violação pode resultar em um alto risco de afetar adversamente os direitos individuais e liberdades civis de acordo com a legislação de proteção de dados;
- b) se a notificação ajudaria o(s) indivíduo(s) afetado(s) (por exemplo, eles poderiam agir para mitigar riscos?);
- c) se a notificação ajudaria a prevenir o uso não autorizado ou ilegal de dados;
- d) se há quaisquer requisitos de notificação legal ou contratual, entre outros fatores.

As pessoas cujos dados pessoais foram afetados pelo incidente serão notificadas quando for considerado provável que resulte em um alto risco de afetar adversamente os direitos e liberdades desse indivíduo, sendo informadas sem demora injustificada. A notificação incluirá uma descrição de como e quando a violação ocorreu e quais os dados envolvidos. Será dada orientação clara e específica sobre o que eles podem fazer para se protegerem e incluir as ações já tomadas para mitigar os riscos.

As pessoas também poderão entrar em contato com a Companhia para mais informações ou para fazer perguntas sobre o que aconteceu, por intermédio do DPO no e-mail [privacidade@interconstrutora.com.br](mailto:privacidade@interconstrutora.com.br).

O LIO e/ou o DPO deve considerar notificar terceiros, como a polícia, seguradoras, bancos ou empresas de cartão de crédito. Isso seria apropriado onde atividades ilegais são conhecidas ou se acredita ter ocorrido, ou onde existe o risco de que atividades ilegais possam ocorrer no futuro.

O LIO e/ou o DPO irá considerar se a Assessoria de Imprensa/Comunicação deve ser informada para elaboração de um eventual comunicado à imprensa e para estar pronta para lidar com quaisquer solicitações recebidas desta.

Será mantido registro de qualquer incidente de segurança da informação e/ou violação de dados pessoais, independentemente da necessidade de notificação.

## 9. Avaliação e resposta

Uma vez que o incidente inicial seja contido, o DPO e/ou o responsável pela SI irão realizar uma revisão completa das causas da violação, a eficácia da(s) resposta(s) e se há alterações nos sistemas, políticas e procedimentos que devem ser realizados.

Os controles existentes serão revisados para determinar sua adequação e se há alguma ação corretiva que deva ser tomada para minimizar o risco de ocorrência de incidentes semelhantes.

A revisão referida considerará:

- a) onde e como as informações e dados pessoais são mantidos e onde e como são armazenados;
- b) onde estão os maiores riscos, incluindo a identificação de potenciais pontos fracos dentro das medidas de segurança existentes;
- c) se os métodos de transmissão de informações são seguros;
- d) se se compartilha uma quantidade mínima de dados necessários;
- e) conscientização da equipe;
- f) implementar um plano de violação de ativos de informação e identificar um grupo de indivíduos responsáveis por reagir às violações de segurança relatadas.

Se necessário, um relatório recomendando quaisquer mudanças nos sistemas, políticas e procedimentos será avaliado pela Direção Executiva da Companhia.

## 10. Violação e penalidades

As infrações ocorridas violando as normas que compõem a Política de Resposta a Incidentes de Segurança da Informação deverão ser analisadas pelo gestor imediato do infrator, que deverá comunicar imediatamente a TI para fins de determinação da apuração das eventuais responsabilidades dos Colaboradores envolvidos.

Caso as infrações sejam realizadas por fornecedores, prestadores de serviço e/ou agentes externos, os casos serão apurados pelos setores de Tecnologia da Informação e Jurídico, para determinação das providências cabíveis.

Em caso de dúvidas entrar em contato com o setor de Tecnologia da Informação através do e-mail [segurancadainformacao@interconstrutora.com.br](mailto:segurancadainformacao@interconstrutora.com.br).

## **11. Revisão desta Política**

Esta Política será atualizada conforme necessário para refletir as melhores práticas e para garantir a conformidade com quaisquer alterações ou emendas à legislação pertinente.

## ANEXO 01

### FORMULÁRIO PARA RELATAR INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Aja imediatamente para relatar quaisquer violações de ativo de informação. Se você descobrir uma violação de informação e/ou dados pessoais, notifique o seu gestor imediatamente, preencha a Seção 1 deste formulário e envie-o por e-mail para o Gestor de TI ([segurancadainformacao@interconstrutora.com.br](mailto:segurancadainformacao@interconstrutora.com.br)) e o Encarregado de Tratamento de Dados Pessoais (DPO) ([privacidade@interconstrutora.com.br](mailto:privacidade@interconstrutora.com.br)) quando apropriado. Há uma versão deste formulário em formato eletrônico na Intranet.

<b>Seção 1: Notificação de violação de segurança da informação</b>	<b>A ser preenchida pelo gestor da pessoa que está relatando o incidente</b>
Data de descoberta do incidente:	
Data(s) do incidente:	
Lugar do incidente:	
Nome da pessoa que está reportando o incidente:	
Contatos da pessoa que está reportando o incidente:	
Breve descrição do incidente ou detalhes da informação perdida:	
Número de titulares de dados afetados, se conhecido:	
Algum dado pessoal foi colocado em risco? Se sim, forneça detalhes:	
Breve descrição de qualquer ação realizada no momento de descoberta:	
<b>PARA USO DO ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS (DPO) e/ou GESTOR DE TI</b>	
Recebido por:	
Data do recebimento:	
Encaminhado para ação de:	
Data do encaminhamento	

<b>Seção 2: Avaliação de gravidade</b>	<b>A ser preenchido pelo Chefe de Investigação (LIO) em consulta com o gestor da área afetada pela violação e, se apropriado, o Gestor de TI, quando aplicável.</b>
<b>Detalhes dos sistemas de TI, equipamentos, dispositivos, registros envolvidos no incidente de segurança:</b>	
<b>Detalhes da informação perdida</b>	
Qual a natureza da informação perdida?	
Quantos dados foram perdidos? Se o laptop for perdido ou roubado: quão recentemente foi feito o backup do laptop no Setor de TI?	
A informação é única? Sua perda terá efeitos adversos na operação, financeiro, legal, ou consequências para a reputação da Companhia ou terceiros?	
Quantos titulares de dados foram afetados?	
Os dados estão vinculados a algum contrato de seguro?	
Qual é a natureza da sensibilidade dos dados? Forneça detalhes de qualquer tipo de informação que se enquadra em qualquer uma das seguintes categorias:	
Dados pessoais de ALTO RISCO - Categorias especiais de dados pessoais (conforme definido na Lei Geral de Proteção de Dados) relativa a uma pessoa a) origem racial ou étnica; b) opiniões políticas ou crenças religiosas; c) filiação sindical; d) genética; e) biometria (quando usado para fins de identificação) f) saúde; g) vida sexual ou orientação sexual.	
- Informações que podem ser usadas para cometer fraude de identidade, como: conta bancária pessoal e outras informações financeiras; identificadores nacionais, como CPF, RG e CTPS;	
- Informações pessoais relacionadas a adultos vulneráveis e crianças ou adolescentes;	
- Perfis detalhados de indivíduos, incluindo informações sobre desempenho de trabalho, salários ou vida pessoal que causaria danos significativos para essa pessoa se divulgada;	
Informações de segurança que comprometeriam o segurança dos indivíduos, se divulgada;	

Informações estratégicas da Companhia, como aquisições de terrenos, descrição de projetos, dados financeiros da Companhia, entre outros.	
<b>PARA USO DO ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS (DPO) e do LIO</b>	
DPO e/ou o LIO deve considerar se deve ser encaminhado para a Direção Executiva da Companhia	

<b>Seção 3: Medida tomada</b>	<b>A ser preenchido pelo DPO e/ou LIO</b>
Número do incidente	p.ex. 2020/001
Incidente reportado por:	
Data em que foi reportado:	
Ação tomada pelo(s) gestor(es) responsável(is):	
O incidente foi reportado para a autoridade policial:	Sim ou não: Se sim, quando: Se sim, apresentar cópia do Boletim de Ocorrência
Ação de acompanhamento necessária/recomendada:	
Reportado ao DPO e /ou ao LIO em:	
Reportado a outras partes interessadas internas (detalhes, datas):	

<b>PARA USO DO ENCARREGADO DE TRATAMENTO DE DADOS PESSOAIS (DPO) e/ou LIO</b>	
Notificação para a ANPD:	Sim ou Não: Se sim, quando: Detalhes:
Notificação para os titulares de dados pessoais:	Sim ou Não: Se sim, quando: Detalhes:
Notificação para outro ente externo, regulador ou parte interessada (p.ex. MP, PROCON, entre outros)	Sim ou Não: Se sim, quando: Detalhes:

# Política de Segurança da Informação

---

GRUPO INTER



## Sumário

<b>Glossário</b> .....	3
<b>1. Introdução</b> .....	5
<b>2. Objetivo</b> .....	5
<b>3. Abrangência</b> .....	5
<b>4. Responsabilidades</b> .....	5
<b>I – Colaboradores e Prestadores de Serviços</b> .....	5
<b>II – Gestores</b> .....	6
<b>III – Segurança da Informação</b> .....	6
<b>IV – Tecnologias da Informação</b> .....	7
<b>V – Gestor da TI</b> .....	7
<b>VI – Departamento Pessoal e Recursos Humanos</b> .....	7
<b>5. Classificação das informações</b> .....	7
<b>I - Dados pessoais</b> .....	7
<b>II – Pública</b> .....	8
<b>III – Interna</b> .....	8
<b>IV – Confidencial</b> .....	8
<b>V - Confidencial Restrita</b> .....	8
<b>6. Comunicação de incidentes da segurança da informação</b> .....	9
<b>7. Solicitações de serviços para o setor de TI</b> .....	9
<b>8. Divulgação de informações</b> .....	9
<b>9. Uso da estação de trabalho</b> .....	9
<b>10. Utilização da rede e sistemas</b> .....	10
<b>I - Rede</b> .....	10
<b>II - Armazenamento na Rede</b> .....	11
<b>III - Acesso aos Sistemas e/ou Acesso externo à Rede interna</b> .....	12
<b>11. Utilização de e-mail</b> .....	12
<b>12. Segurança física e lógica</b> .....	13
<b>13. Senhas</b> .....	14
<b>14. Dispositivos particulares</b> .....	15
<b>15. Computadores e dispositivos fornecidos pela Companhia</b> .....	15
<b>16. Impressoras e documentos impressos</b> .....	15
<b>17. Controle de Acessos</b> .....	16

**18. Violação e penalidades ..... 16**

## Glossário

- a) Ativo de informação – informações essenciais para os negócios da empresa passíveis de valoração.
- b) CSC (Central de Serviços Compartilhados) – Sistema onde são geridos os atendimentos e demandas e comunicação entre os setores e serviços.
- c) Códigos maliciosos – são programas de computador cujo objetivo é infiltrar-se ilicitamente em um sistema alheio para causar danos, alterações ou roubar informações.
- d) Confidencialidade da informação – quando a informação não está disponível ou revelada a quem não tenha autorização para acessá-la.
- e) Dados pessoais – são informações vinculadas à uma pessoa natural e que podem identificá-la de alguma forma, como por exemplo o nome, número de CPF ou RG, endereço etc.
- f) Disponibilidade da informação – quando a informação está acessível e utilizável quando solicitada por alguém que tenha autorização para acessá-la.
- g) Evento de segurança da informação – Trata-se de uma ocorrência identificada de um estado de sistema, serviço ou rede, que indique a possibilidade de violação da política de segurança da informação ou uma falha de controles, ou ainda uma situação desconhecida, que seja relevante para a segurança da informação.
- h) Incidente de segurança da informação – Um ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- i) Integridade da informação – quando é resguardada a exatidão e completeza da informação.
- j) *Mail bombing* – forma de ataque a uma determinada conta de e-mail, quando são enviadas a ela uma grande quantidade de mensagens, visando prejudicar o acesso a recursos digitais.
- k) Segurança da informação ou SI – quando são implementadas ações que visam proteger a confidencialidade, integridade e disponibilidade da informação. Estas ações também podem visar a preservação da autenticidade, responsabilidade, não repúdio e confiabilidade.
- l) Segurança física – forma de proteger equipamentos e informações contra acessos indevidos, bem como assegurar a integridade e disponibilidade das informações.
- m) Segurança lógica – forma de controlar o acesso a aplicativos, dados, sistemas operacionais, senhas e arquivos de *log*, utilizando-se de *firewalls*, criptografia, antivírus, entre outras.
- n) *Spam* – são mensagens de e-mail geralmente enviadas para um grande número de pessoas que não as solicitaram.
- o) Tratamento de dados pessoais – qualquer operação realizada com dados pessoais. Tais como coleta, recepção, transmissão, acesso, reprodução, armazenamento, arquivamento, entre outras.

**p)** Vazamento de dados – incidente de segurança da informação que tenha provocado a disponibilidade de dados pessoais para quem não tem autorização para acessá-los.

## 1. Introdução

A Política de Segurança da Informação (“**Política**” ou “**PSI**”) da Inter Construtora e Incorporadora S.A. (“**Companhia**”) é o documento responsável por estabelecer e direcionar as atividades que envolvam o tratamento de informações dentro da organização, protegendo ativos e prevenindo responsabilidades.

Foi elaborada levando em consideração as principais normas de padronização, como ISO/ABNT 27001, 27002 e 27701, além de normas legais como a Lei Geral de Proteção de Dados (Lei n. 13.709/2018).

Esta Política deve ser observada por todas as áreas da organização, sendo objeto de campanhas regulares de conscientização e disseminação.

Esta versão está sujeita a alterações periódicas e sempre que for necessária sua adaptação a novos regulamentos e boas práticas.

## 2. Objetivo

Esta Política tem como objetivo estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações assim como complementar a Política de Proteção de Dados e Privacidade, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- A confiabilidade das informações através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa;
- O compromisso da empresa com a proteção das informações de sua propriedade e/ou sob sua guarda;
- A participação e cumprimento por todos os colaboradores em todos os processos.
- O sigilo e a proteção de dados pessoais tratados pela Companhia.

## 3. Abrangência

Esta Política se aplica a todos os colaboradores, empregados, fornecedores, acionistas, e quaisquer pessoas ou empresas que, de alguma, forma façam uso dos sistemas de informação tanto físicos quanto lógicos, utilizados pela Companhia ou tenham algum tipo de interação com eles.

## 4. Responsabilidades

### I – Colaboradores

É de inteira responsabilidade dos colaboradores sendo eles empregados, estagiários, prestador de serviços, gestores, consultores e acionistas:

- Cumprir rigorosamente as políticas, normas e procedimentos de segurança da Companhia;

- Comunicar prontamente ao gestor imediato ou diretamente ao setor de T.I. (Segurança da Informação) qualquer violação destas normas e procedimentos;
- Proteger as informações contra acesso, vazamento, divulgação, modificação ou exclusão conforme o “Termo de Confidencialidade”.
- Caso seja necessário esclarecer dúvidas, deverá ser consultado o setor de T.I.

## **II – Gestores**

Aos gestores ficam as seguintes responsabilidades:

- Ter postura exemplar em relação à segurança da informação, servindo de modelo de conduta para os colaboradores sob sua liderança;
- Cumprir e verificar se os colaboradores sob sua liderança estão cumprindo a PSI, normas e processos de segurança sempre;
- Manter atualizadas as informações sobre processos e/ou cadastros de funcionários, como troca de função por exemplo, junto ao setor de TI, para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade, e para que a segurança das informações envolvidas esteja sempre de acordo;
- Exigir de parceiros, prestadores de serviços, e outras entidades externas o cumprimento das cláusulas contratuais referentes à confidencialidade e segurança da informação;
- Sugerir melhorias nos processos de segurança da informação nas suas respectivas áreas de atuação junto ao setor de TI;
- Reportar qualquer falha ou possível quebra de segurança imediatamente ao setor de TI por meio de formulário eletrônico próprio disponível na Intranet.

## **III – Segurança da Informação**

Aos profissionais das áreas de T.I. e Segurança da Informação ficam designadas as seguintes responsabilidades:

- Verificar e propor melhorias contínuas para a PSI, processos e normas;
- Executar ações preventivas e corretivas adequadas;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.

#### **IV – Tecnologias da Informação**

Ao setor de TI ficam as seguintes responsabilidades:

- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede, computadores etc.), tendo como referência a PSI;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações.

#### **V – Gestor da TI**

Ao Gestor da área de Tecnologia da Informação ficam as seguintes responsabilidades:

- Propor melhorias, alterações e ajustes da PSI;
- Propor campanhas de conscientização e sensibilização;
- Propor ações preventivas e corretivas adequadas;
- Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
- Classificar e reclassificar o nível de acesso às informações sempre que necessário;
- Avaliar incidentes de segurança e propor ações corretivas;
- Realizar auditorias internas para verificação da eficácia da presente PSI.

#### **VI – Departamento Pessoal e Recursos Humanos**

- O setor de Recursos Humanos ficará responsável por dar ciência formalizada e disponibilizar o acesso à PSI para os colaboradores na fase de contratação e formalização do trabalho e em posteriores alterações da PSI;
- O setor de Departamento Pessoal ficará responsável por dar ciência ao setor de TI de eventos críticos relacionados ao colaborador, como desligamento, baixa, férias, afastamento etc. assim que o mesmo ocorrer, para que as devidas providências de bloqueios de acesso e cancelamento de usuário e serviços utilizados pelo colaborador possam ser realizados.

## **5. Classificação das informações**

### **I - Dados pessoais**

São informações relativas a uma pessoa viva, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa. Neste documento serão tratadas as normas e regras para manter estas informações em segurança. Para mais informações e detalhes, verificar a Política de Proteção de Dados e Privacidade. São exemplos de dados pessoais:

- O endereço de uma residência;

- Nome e apelido;
- Atestado médico;
- Endereço IP ou cookies de navegação;

## **II – Pública**

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

São exemplos de informação pública:

- Informações que estão disponibilizadas no site para o cliente;
- Planta Humanizada;
- Fotos do empreendimento;

## **III – Interna**

São informações disponíveis aos colaboradores e prestadores de serviços da Companhia para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

São exemplos de informações internas:

- E-mails e lista telefônica internos;
- Organogramas;
- Políticas e Procedimentos internos;

## **IV – Confidencial**

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

São exemplos de informações confidenciais:

- Contratos com fornecedores;
- Projetos;
- Dados cadastrais de funcionários;

## **V - Confidencial Restrita**

São informações de acesso restrito a um colaborador ou grupo de colaboradores que obrigatoriamente contam como destinatários da mesma, em geral, associadas ao interesse estratégico da empresa e restritas aos gestores, presidência e funcionários cujas funções requeiram conhecê-las.

São exemplos de informações confidenciais restritas:

- Atas de reunião do conselho com presidência e alta cúpula de gestão;
- Indicadores e estatísticas dos processos de negócio da Companhia;

- Resultado de auditorias internas.

## **6. Comunicação de incidentes da segurança da informação**

Quando for preciso comunicar algum incidente de segurança da informação é necessário fazer esta comunicação por meio do formulário eletrônico próprio na Intranet (<https://ptlitnt.interconstrutora.com.br/index.php/pt/incidente-seguranca>).

## **7. Solicitações de serviços para o setor de TI**

No caso da necessidade de realizar alguma solicitação para a equipe de TI envolvendo suporte, dúvidas, dentre outros, dispomos de uma CSC no seguinte endereço: <http://cs.interconstrutora.com.br/>.

Na CSC são mostradas todas as interações e acompanhamentos dos chamados, é o elo de comunicação e atendimento entre os setores de TI, tanto internamente, como com os demais setores da Companhia. Caso não possua usuário cadastrado na Intranet ou na CSC, o gestor deverá solicitar a criação.

## **8. Divulgação de informações**

É proibida a divulgação e/ou o compartilhamento indevido de dados pessoais, informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos (p.ex. WhatsApp) ou qualquer outra tecnologia correlata que use a internet ou outro meio de comunicação como via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei.

O sigilo às informações deve ser sempre praticado de acordo com as normas descritas tanto deste documento quanto no Termo de Confidencialidade.

Apenas colaboradores devidamente autorizados a falar em nome da Companhia para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevista on-line, documento físico, ligação telefônica etc.

Não se aplica o aqui disposto às comunicações decorrentes exclusivamente das atividades laborais do colaborador desde que realizada por meio dos canais oficialmente estabelecidos pela Companhia.

## **9. Uso da estação de trabalho**

Cada computador possui códigos internos os quais permitem que seja identificado na rede. Sendo assim, tudo que for executado será de responsabilidade do usuário.

O computador disponibilizado pela Companhia deverá ser utilizado apenas para a realização das tarefas acordadas e contratadas.

O usuário poderá criar, transmitir, distribuir, disponibilizar e armazenar documentos de acordo com suas funções e sigilo dos dados e informações conforme item 3 deste documento.

Antes de ausentar-se do seu local de trabalho, o usuário deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, e efetuar o *logout/logoff* da rede ou bloqueio do computador através de senha.

Deverá também guardar documentos impressos, não podendo deixar documentos sob a mesa enquanto se ausentar.

Qualquer tipo de *software*, jogos, ou aplicativos e similares não podem ser gravados ou instalados no diretório pessoal do usuário, no computador local ou em qualquer outro diretório da rede.

Caso seja necessário a instalação de algum *software* em específico, o usuário deverá solicitá-la ao setor de TI por meio de um chamado na CSC. O procedimento é o mesmo para remoção e/ou desinstalação.

Fica expressamente proibido:

- Introduzir códigos maliciosos nos sistemas;
- Permitir utilização do computador por prestadores de serviços e terceiros não vinculados à Companhia;
- Acessar ou armazenar qualquer material de cunho pessoal;
- Acessar ou armazenar qualquer material de natureza pornográfica, racista ou criminosa;
- Conectar qualquer equipamento ou periférico não fornecido e/ou não autorizado e/ou não homologado pelo setor de TI;
- O uso, a cópia ou a distribuição não autorizada de *softwares* que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo setor de TI;
- Caso o computador ou dispositivo necessite de reparo solicitar apenas junto à equipe de infraestrutura de TI.

## **10. Utilização da rede e sistemas**

Este tópico trata da utilização da rede e dos sistemas, com os seguintes subtópicos:

### I - Rede

A rede deverá ser utilizada única e exclusivamente para acesso aos sistemas, dados e informações relacionados às atividades executadas pela Companhia.

Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da Companhia, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento desta Política.

Apenas usuários autorizados podem acessar a rede e/ou a internet. Não serão permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta.

Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

A Companhia se reserva ao direito de monitorar e registrar todo o tráfego de rede, computadores e sistemas utilizados e veiculados na empresa, assim como o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, adotar as medidas legais cabíveis e punir os infratores, no caso de uso indevido de recursos.

Uso da internet está sujeito a monitoramento, e o acesso a páginas indevidas de natureza pornográfica, racista, violenta ou criminosa são expressamente proibidos.

## II - Armazenamento na Rede

Caso seja disponibilizado um diretório na rede para o usuário, ele deverá realizar manutenções periodicamente evitando o acúmulo de informações desnecessárias.

Materiais de natureza pornográfica, racista, violenta ou criminosa são expressamente proibidos, não poderão ser armazenados, distribuídos, editados ou gravados através do uso dos recursos computacionais da rede.

A rede deve ser apenas e unicamente utilizada para o tráfego de arquivos e dados relacionados diretamente às atividades desempenhadas pela Companhia.

A pasta “PÚBLICA” ou similar, não deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza específica. Ela deve ser utilizada apenas para armazenar informações de interesse geral.

Será feita semanalmente a limpeza dos arquivos armazenados na pasta “PÚBLICA” ou similar, para que não haja acúmulo desnecessário de informações e degradação do acesso ao ambiente de rede.

É obrigatório armazenar os arquivos inerentes à empresa no servidor de arquivos, mantendo-os sempre atualizados, para garantir a cópia de segurança.

É expressamente proibido armazenar dados, informações e documentos pertencentes à Companhia em nuvens/servidores não autorizadas pela TI, como por exemplo algum serviço de armazenamento on-line privado como Google Drive, Dropbox e similares.

### III - Acesso aos Sistemas e/ou Acesso externo à Rede interna

Para que se mantenha a segurança e controle dos dados e informações, quando o colaborador estiver utilizando uma rede localizada fora da Companhia, o acesso à rede de arquivos e servidores deverá ser exclusivamente por meio de uma VPN. Não será possível acessar nenhum destes sistemas caso a VPN não estiver conectada.

Para autorização do acesso via VPN será necessária a solicitação pelo superior direto à TI por meio da CSC, e estará sujeito à aprovação. Caso seja aprovado, o acesso será liberado e configurado.

Todo o tráfego realizado por meio da VPN está sujeito ao monitoramento da Companhia.

## 11. Utilização de e-mail

Fica proibido aos colaboradores e/ou a quem se destinar a utilização do correio eletrônico da Companhia:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da Companhia;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Companhia ou suas unidades vulneráveis a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Produzir, transmitir ou divulgar mensagem que:
  - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Companhia;
  - Contenha ameaças eletrônicas, como: *spam*, *mail bombing*, vírus de computador;
  - Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
  - Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
  - Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

- Fazer uso pessoal da conta de e-mail corporativo.

A conta de e-mail corporativa é considerada ferramenta de trabalho e está sujeita à monitoramento pela Companhia.

As mensagens de correio eletrônico sempre deverão incluir assinatura, estando de acordo com o padrão vigente da empresa, e ficará disponível para todos os colaboradores na Intranet.

## **12. Segurança física e lógica**

Para acesso às dependências de toda empresa é necessário identificação por crachá.

Todas as salas deverão permanecer fechadas, e cada colaborador deverá possuir uma *tag* que o permita transitar pelas áreas atribuídas às suas funções.

A segurança lógica é feita através de diversos mecanismos, desde o uso antivírus e *firewalls* a sistemas mais complexos de controle, monitoramento e segurança.

Os servidores físicos proprietários estão em uma sala protegida dentro da Companhia, o *Data Center*. Todo o acesso a esta sala é monitorado tanto por câmeras quanto por mecanismo de autenticação individual, permanecendo sempre fechada.

Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras do *Data Center*.

O acesso ao *Data Center* só pode ser realizado por pessoas autorizadas. Caso seja necessário o acesso por colaboradores de outras áreas, prestadores de serviços, dentre outros, deverá ser feito sob supervisão e acompanhamento do responsável pela Segurança de TI ou alguém indicado por ele, mediante autorização prévia do setor de Segurança de TI.

O acesso às dependências do *Data Center* com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de segurança e mediante supervisão.

O acesso ao *Data Center* sem as devidas identificações só poderá ocorrer em emergências quando a segurança física do *Data Center* for comprometida, como por incêndio, inundação, abalo da estrutura predial e similares.

O *Data Center* deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

A entrada ou retirada de quaisquer equipamentos do *Data Center* somente se dará por meio de solicitação na CSC e liberação pelo colaborador solicitante e a mesma deve ser autorizada pelo Gestor de Segurança da Informação.

### **13. Senhas**

A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo ser imediatamente alterada no caso de suspeita de sua divulgação.

Caso a senha seja digitada erroneamente quer por erro ou por tentativa de acesso indevida por mais de 03 (três) tentativas o usuário ficará bloqueado, sendo necessário solicitar ao setor de TI o desbloqueio, e o incidente será analisado para verificar se houve alguma quebra de segurança.

A senha inicial ou trocada quando fornecida ao colaborador é padrão, sendo sempre solicitada a troca no primeiro login.

Não poderão ser fornecidas por telefone, comunicador instantâneo ou qualquer outra forma que não assegure a identidade do utilizador do sistema.

Caso o usuário esqueça ou necessite da troca de senha por outro motivo, e não possua e-mail de recuperação corretamente cadastrado, será necessário entrar em contato com o setor de TI e realizar uma solicitação na CSC, com justificativa, e quando necessário provar e validar a identidade do usuário do sistema, para que a senha seja fornecida corretamente ao dono.

É proibido o compartilhamento de *login*, o qual é pessoal e intransferível.

É recomendável utilizar um método próprio para lembrar da senha, de modo que ela não precise ser escrita em nenhum local em hipótese alguma, e se assim for necessário, guardá-la de modo seguro.

Não anotar a senha em papel ou em outros meios de registro de fácil acesso. As senhas não devem ser anotadas e deixadas próximas ao computador (debaixo do teclado, colada no monitor etc.).

As senhas deverão seguir os seguintes pré-requisitos, a serem exigidos para todos os sistemas utilizados pela Companhia:

- Tamanho mínimo de doze caracteres;
- Existência de letras minúsculas, maiúsculas, números e caracteres especiais;
- Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, nome da empresa etc.).

As senhas de todos os sistemas deverão ser atualizadas a cada 45 dias obrigatoriamente.

## **14. Dispositivos particulares**

A utilização de dispositivos particulares é permitida através de autorização do setor de TI, mediante pedido prévio através de solicitação na CSC pelo superior imediato do solicitante. Será assinado um termo de responsabilidade para ciência de ambas as partes.

Dispositivos particulares não receberão manutenção ou atendimento de suporte técnico pela Companhia.

Quando necessário, o proprietário do dispositivo deverá arcar com manutenções corretivas e/ou adequações exigidas pelo setor de TI para autorização do uso do dispositivo.

O dispositivo móvel em questão poderá ter os acessos monitorados ao acessar qualquer um dos sistemas utilizados pela Companhia ou quando conectado nas redes da Companhia.

## **15. Computadores e dispositivos fornecidos pela Companhia**

Os computadores e dispositivos eletrônicos fornecidos pela Companhia para execução das tarefas, deverão ser utilizados preferencialmente dentro das dependências da Companhia.

Caso o colaborador necessite transportar o computador(es) e/ou dispositivo(s) fornecido pela Companhia poderá realizá-lo mediante autorização do superior imediato juntamente ao setor de TI por meio da CSC, formalizando por assinatura do “Termo de Autorização de Transporte de Dispositivo”.

O “Termo de Autorização de Transporte de Dispositivo” poderá permitir ao colaborador transportar o computador e/ou dispositivo por um prazo definido ou enquanto durar o contrato de trabalho, a depender das funções e cargos.

## **16. Impressoras e documentos impressos**

Ao enviar o arquivo para impressão, o colaborador deverá imediatamente verificar se o que foi solicitado já está disponível na impressora, não deixando documentos na bandeja da impressora. Esta norma tem por objetivo evitar que pessoas não autorizadas tenham acesso a documentos recém impressos.

Existe um servidor de controle de serviços de impressão onde colaboradores recebem cotas de impressão e, quando estas são excedidas, é necessária autorização do superior e abertura de chamado na CSC.

Impressos com erro e/ou não mais úteis podem ser utilizados como rascunho caso tratem de informações **públicas** apenas e não contenham nenhum tipo de **dado pessoal**.

Impressos que contenham informações com qualquer tipo de **dados pessoais** ou classificadas como **Interna e/ou Confidencial e/ou Confidencial Restrita** não poderão ser utilizados como rascunho caso sejam impressos com erros ou não tenham mais função. Neste caso deverão ser destruídos imediatamente rasgados ou por meio de picotadora de papel.

Caso o colaborador se ausente da sua estação de trabalho não deverá deixar nenhum documento exposto.

É proibida a impressão e cópia de documentos de cunho pessoal e/ou ilegal.

## **17. Controle de Acessos**

A fim de proteger as informações de acessos indevidos, os sistemas são parametrizados com controles de acessos.

O acesso do usuário deverá ser imediatamente suspenso nas seguintes situações:

- Desligamento, férias, licença ou afastamento do colaborador;
- Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação;
- Quando identificado o não cumprimento das políticas e normas da Companhia.

Para os cancelamentos acima mencionados, o DP ficará responsável por informar prontamente o setor de TI acerca dos desligamentos e os gestores de cada setor responsáveis por informar a mudança de função, bloqueio ou suspensão de acesso dos colaboradores.

## **18. Violação e penalidades**

As infrações ocorridas violando as normas que compõem esta Política deverão ser analisadas pelo gestor imediato do infrator, que deverá comunicar imediatamente a TI para fins de determinação da apuração das eventuais responsabilidades dos funcionários envolvidos.

Caso as infrações sejam realizadas por fornecedores, prestadores de serviço e/ou agentes externos, os casos serão apurados pelos setores de TI e Jurídico, para determinação das providências cabíveis.

Em caso de dúvidas entrar em contato com o setor de TI através do e-mail [segurancadainformacao@interconstrutora.com.br](mailto:segurancadainformacao@interconstrutora.com.br).