

Código Institucional de Ética, Conduta, Integridade, Segurança da Informação e Proteção de Dados

1. Apresentação Institucional

O presente Código Institucional de Ética, Conduta, Integridade, Segurança da Informação e Proteção de Dados estabelece os princípios, valores, diretrizes e responsabilidades que orientam a atuação da organização, de seus profissionais, colaboradores, parceiros, fornecedores e demais partes relacionadas.

A organização atua na prestação de serviços especializados de Consultoria Empresarial, Consultoria e Auditoria de Tecnologia da Informação, Gestão de Riscos, Compliance, Auditoria Interna, Controles Internos, Governança Corporativa, Governança Pública e Cursos e Treinamentos Corporativos.

Em razão da natureza dos serviços prestados, a organização possui acesso a informações estratégicas, dados corporativos, documentos técnicos, relatórios, ambientes tecnológicos, processos internos e informações confidenciais de clientes e instituições públicas.

Dessa forma, a ética, a integridade, a independência profissional, a proteção das informações e o compromisso com a confidencialidade representam fundamentos essenciais para a construção de relações baseadas em confiança e credibilidade.

Este Código estabelece os padrões mínimos de comportamento esperados e orienta decisões profissionais, garantindo que todas as atividades sejam conduzidas de maneira responsável, transparente, segura e alinhada às melhores práticas nacionais e internacionais.

2. Objetivos do Código

Este Código possui como objetivos:

- Estabelecer princípios éticos aplicáveis às atividades profissionais;
- Orientar comportamentos e decisões diante de situações que envolvam dilemas éticos;
- Garantir tratamento adequado das informações acessadas durante os trabalhos;
- Preservar a confidencialidade e segurança dos dados tratados;

- Assegurar independência, imparcialidade e objetividade profissional;
- Prevenir conflitos de interesse, fraudes, corrupção e práticas inadequadas;
- Promover uma cultura organizacional baseada em integridade e responsabilidade;
- Estabelecer diretrizes para proteção de informações corporativas e dados pessoais;
- Reforçar o compromisso institucional com clientes, parceiros e sociedade.

3. Valores Institucionais

A atuação profissional é baseada nos seguintes valores:

3.1 Ética

A organização conduz suas atividades com honestidade, transparência e respeito aos princípios profissionais, legais e regulatórios aplicáveis.

Toda decisão deve considerar não apenas os resultados esperados, mas também os impactos éticos, institucionais e sociais envolvidos.

3.2 Integridade

A integridade representa o compromisso de agir corretamente, mesmo diante de situações de pressão, conflito ou incerteza.

Não são admitidas práticas que comprometam a confiança, a reputação institucional ou a credibilidade dos serviços prestados.

3.3 Excelência Técnica

A qualidade dos serviços prestados depende da competência profissional, atualização contínua e aplicação de metodologias reconhecidas.

A organização busca entregar análises, recomendações e soluções baseadas em conhecimento técnico, evidências e boas práticas.

3.4 Confiança e Responsabilidade

A confiança depositada por clientes e parceiros constitui um patrimônio institucional.

Todos os profissionais possuem responsabilidade direta pela preservação dessa confiança por meio de atitudes éticas, responsáveis e profissionais.

3.5 Independência e Imparcialidade

As atividades de consultoria, auditoria, avaliação e diagnóstico devem ser conduzidas sem interferências indevidas, interesses particulares ou pressões externas.

Opiniões técnicas devem ser fundamentadas exclusivamente em fatos, evidências e critérios profissionais.

4. Aplicabilidade

Este Código aplica-se a:

- Sócios e administradores;
- Consultores;
- Auditores;
- Instrutores;
- Colaboradores internos;
- Prestadores de serviços;
- Parceiros estratégicos;
- Terceiros que atuem em nome da organização.

Todos possuem responsabilidade individual pelo conhecimento, cumprimento e disseminação dos princípios estabelecidos neste documento.

5. Princípios de Conduta Profissional

5.1 Respeito às Pessoas

A organização valoriza relações profissionais baseadas em respeito, colaboração, cordialidade e dignidade.

Não são aceitas práticas de discriminação, assédio, intimidação, constrangimento ou qualquer comportamento incompatível com um ambiente profissional saudável.

5.2 Responsabilidade Profissional

Cada profissional deve atuar com responsabilidade, zelo e comprometimento, assumindo as consequências de suas decisões e entregas.

São esperadas atitudes como:

- Cumprimento de compromissos assumidos;
- Comunicação clara e transparente;
- Registro adequado de informações relevantes;
- Preservação da qualidade técnica dos trabalhos;
- Respeito aos prazos acordados.

5.3 Competência e Atualização Profissional

Os profissionais devem manter conhecimento atualizado sobre:

- Normas técnicas;
- Legislações aplicáveis;
- Frameworks de mercado;
- Tecnologias utilizadas;
- Metodologias profissionais;
- Boas práticas relacionadas às áreas de atuação.

A organização incentiva permanentemente o desenvolvimento profissional e a disseminação do conhecimento.

6. Compromisso com Clientes e Instituições

A relação com clientes e instituições atendidas deve ser pautada por:

- Transparência;
- Respeito;
- Confidencialidade;
- Independência técnica;
- Qualidade profissional;
- Cumprimento dos compromissos estabelecidos.

A organização compromete-se a não emitir relatórios, diagnósticos ou recomendações influenciadas por interesses externos ou solicitações que comprometam critérios técnicos.

Todas as conclusões profissionais devem representar fielmente os fatos analisados e as evidências obtidas durante os trabalhos.

7. Independência e Objetividade Profissional

A independência profissional constitui um princípio fundamental para a execução de serviços de consultoria, auditoria, avaliação, diagnóstico e capacitação.

A organização compromete-se a conduzir todas as atividades com autonomia técnica, imparcialidade e objetividade, assegurando que análises, conclusões e recomendações sejam baseadas em critérios profissionais, evidências obtidas durante os trabalhos e metodologias reconhecidas.

Nenhum profissional deve permitir que interesses pessoais, financeiros, comerciais ou externos influenciem julgamentos técnicos ou comprometam a qualidade das entregas realizadas.

A independência deve ser preservada não apenas em situações reais de conflito, mas também em circunstâncias que possam gerar percepção de falta de imparcialidade perante clientes, parceiros ou demais partes interessadas.

7.1 Responsabilidades Relacionadas à Independência

Todos os profissionais envolvidos nos trabalhos devem:

- Avaliar previamente potenciais situações que possam comprometer sua independência;
- Comunicar qualquer circunstância que possa representar conflito de interesse;
- Evitar participação em atividades incompatíveis com a imparcialidade necessária;
- Manter postura técnica e profissional diante de pressões externas;
- Registrar limitações ou restrições que possam afetar a execução dos trabalhos.

A organização poderá realizar avaliações internas de independência sempre que necessário, especialmente em projetos envolvendo auditoria, avaliação de controles, compliance, riscos ou ambientes regulados.

8. Conflitos de Interesse

Conflito de interesse ocorre quando interesses pessoais, financeiros, profissionais ou relacionamentos externos possam interferir, ou aparentar interferir, na capacidade de atuação objetiva e independente.

A existência de um potencial conflito não representa necessariamente uma irregularidade, porém exige identificação, comunicação, análise e tratamento adequado.

8.1 Exemplos de Situações de Conflito de Interesse

Podem caracterizar potenciais conflitos:

- Possuir relação pessoal próxima com representantes da organização avaliada;
- Ter interesse financeiro direto ou indireto em clientes ou fornecedores envolvidos;
- Participar de decisões relacionadas a organizações nas quais exista interesse particular;
- Utilizar informações obtidas durante trabalhos profissionais para benefício próprio;
- Atuar simultaneamente em atividades incompatíveis;
- Receber benefícios capazes de influenciar decisões profissionais.

8.2 Tratamento de Conflitos de Interesse

Todos os profissionais devem comunicar situações reais ou potenciais de conflito de interesse antes do início ou durante a execução dos trabalhos.

A organização avaliará cada situação considerando:

- Natureza do conflito;
- Impacto na independência profissional;
- Riscos para o cliente e para a organização;
- Possibilidade de implementação de controles mitigadores.

Quando não for possível eliminar ou reduzir adequadamente o conflito, a organização poderá recusar, interromper ou redirecionar a participação no trabalho.

9. Confidencialidade e Sigilo Profissional

A confidencialidade representa um dos compromissos fundamentais da organização, considerando a natureza estratégica das informações acessadas durante a execução dos serviços.

Os profissionais podem ter contato com informações financeiras, operacionais, estratégicas, tecnológicas, jurídicas, administrativas, pessoais e institucionais pertencentes aos clientes e parceiros.

Todas essas informações devem ser tratadas como confidenciais e protegidas contra acesso, uso, divulgação ou compartilhamento não autorizado.

9.1 Princípios de Confidencialidade

Os profissionais devem:

- Utilizar informações exclusivamente para finalidades relacionadas aos trabalhos contratados;
- Compartilhar informações somente com pessoas autorizadas;
- Manter documentos protegidos durante e após a execução dos serviços;
- Evitar discussões sobre informações confidenciais em ambientes inadequados;
- Adotar cuidados especiais em comunicações eletrônicas;

- Respeitar acordos de confidencialidade firmados com clientes e parceiros.

9.2 Informações Consideradas Confidenciais

São consideradas confidenciais, entre outras:

- Estratégias empresariais;
- Planejamentos organizacionais;
- Relatórios técnicos;
- Papéis de trabalho de auditoria;
- Diagnósticos e avaliações realizadas;
- Informações financeiras;
- Dados de clientes, fornecedores e colaboradores;
- Arquiteturas de sistemas;
- Configurações tecnológicas;
- Vulnerabilidades identificadas;
- Políticas internas;
- Processos operacionais;
- Informações obtidas durante entrevistas e levantamentos.

9.3 Permanência do Dever de Sigilo

A obrigação de confidencialidade permanece válida mesmo após:

- Encerramento do contrato;
- Finalização dos projetos;
- Desligamento de profissionais;
- Encerramento de relacionamentos comerciais.

A utilização indevida de informações obtidas durante atividades profissionais constitui violação grave deste Código.

10. Segurança da Informação

A organização reconhece que a proteção da informação é essencial para garantir a confiabilidade dos serviços prestados e preservar os interesses dos clientes, parceiros e demais partes relacionadas.

A segurança da informação deve ser baseada nos princípios fundamentais de:

Confidencialidade

Garantia de que informações sejam acessadas somente por pessoas autorizadas.

Integridade

Garantia de que informações permaneçam completas, corretas e protegidas contra alterações indevidas.

Disponibilidade

Garantia de que informações e recursos estejam disponíveis quando necessários para execução adequada das atividades.

11. Diretrizes de Segurança da Informação

Todos os profissionais devem adotar medidas adequadas para proteção das informações, incluindo:

- Utilização de senhas individuais e seguras;
- Proteção de credenciais de acesso;
- Bloqueio de equipamentos quando não estiverem em uso;
- Armazenamento seguro de documentos;
- Uso responsável de dispositivos corporativos;
- Restrição de compartilhamento de arquivos;
- Utilização de ferramentas autorizadas;
- Comunicação imediata de incidentes ou suspeitas de comprometimento.

É proibido:

- Compartilhar credenciais pessoais;
- Copiar informações confidenciais sem autorização;

- Utilizar informações profissionais para benefício pessoal;
- Armazenar documentos corporativos em ambientes não autorizados;
- Encaminhar informações sensíveis para destinatários incorretos.

12. Classificação e Tratamento das Informações

As informações tratadas pela organização devem ser classificadas conforme seu nível de sensibilidade e criticidade.

A classificação pode considerar:

Pública

Informações autorizadas para divulgação externa.

Interna

Informações destinadas exclusivamente ao uso organizacional.

Confidencial

Informações cujo acesso deve ser restrito a pessoas autorizadas.

Restrita

Informações críticas, estratégicas ou sensíveis, cujo acesso indevido pode gerar impactos relevantes.

O tratamento das informações deve respeitar o nível de classificação definido, aplicando controles compatíveis com o grau de sensibilidade.

13. Proteção de Dados Pessoais e Privacidade

A organização reconhece a importância da proteção dos dados pessoais e assume compromisso com o tratamento responsável das informações relacionadas a pessoas físicas.

O tratamento de dados pessoais deve observar os princípios previstos na legislação aplicável, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo:

- Finalidade;
- Adequação;

- Necessidade;
- Transparência;
- Segurança;
- Prevenção;
- Não discriminação;
- Responsabilização.

13.1 Diretrizes para Tratamento de Dados Pessoais

Os profissionais devem:

- Utilizar dados pessoais somente para finalidades autorizadas;
- Coletar apenas informações necessárias ao trabalho;
- Proteger dados contra acesso indevido;
- Evitar compartilhamentos sem autorização;
- Respeitar direitos dos titulares dos dados;
- Comunicar incidentes envolvendo dados pessoais.

13.2 Dados Sensíveis

Dados pessoais sensíveis devem receber tratamento especial devido ao potencial impacto sobre a privacidade dos titulares.

O acesso deve ser limitado estritamente às pessoas autorizadas e somente quando necessário para execução das atividades profissionais.

14. Compromisso com a Privacidade

A organização busca estabelecer uma cultura permanente de proteção da privacidade, garantindo que informações pessoais e corporativas sejam tratadas com responsabilidade, segurança e respeito.

Todos os profissionais possuem papel fundamental na proteção das informações confiadas à organização.

15. Integridade e Combate à Corrupção

A organização mantém compromisso permanente com a ética, a integridade e o cumprimento das legislações aplicáveis, não tolerando qualquer prática que envolva corrupção, fraude, suborno, favorecimento indevido ou qualquer conduta que comprometa a transparência e a legitimidade das relações profissionais.

Todas as atividades devem ser conduzidas de forma honesta, transparente e responsável, respeitando os princípios de legalidade, moralidade, impessoalidade e boa-fé.

A organização repudia qualquer tentativa de obtenção de vantagens indevidas, seja em relacionamentos com clientes, fornecedores, parceiros, agentes públicos ou quaisquer outras partes interessadas.

16. Práticas Proibidas

São expressamente proibidas quaisquer práticas relacionadas a:

- Pagamentos indevidos ou facilitação de processos por meios ilegítimos;
- Oferta, promessa ou recebimento de vantagens indevidas;
- Manipulação de informações, documentos ou resultados;
- Falsificação de relatórios, registros ou evidências;
- Ocultação deliberada de informações relevantes;
- Apropriação indevida de recursos ou informações;
- Uso de informações privilegiadas para benefício pessoal;
- Interferência indevida em processos de decisão;
- Qualquer conduta que possa caracterizar corrupção ou fraude.

A violação desses princípios poderá resultar em medidas administrativas, contratuais e legais aplicáveis.

17. Relacionamento com Clientes

O relacionamento com clientes deve ser construído com base em confiança, transparência, respeito e compromisso com a excelência profissional.

A organização compromete-se a:

- Prestar serviços com qualidade técnica;
- Cumprir os compromissos assumidos;
- Manter comunicação clara e profissional;
- Preservar informações confidenciais;
- Atuar com independência e imparcialidade;
- Apresentar avaliações e recomendações fundamentadas em critérios técnicos.

A organização não deve aceitar solicitações que impliquem:

- Manipulação de resultados;
- Omissão de informações relevantes;
- Alteração indevida de conclusões técnicas;
- Emissão de opiniões sem fundamentação adequada.

A preservação da independência profissional deve prevalecer mesmo diante de interesses comerciais ou pressões externas.

18. Relacionamento com Fornecedores e Parceiros

A seleção e relacionamento com fornecedores e parceiros devem observar critérios de ética, transparência, competência técnica e capacidade de entrega.

A organização busca estabelecer relações profissionais sustentáveis, baseadas em:

- Confiança;
- Respeito mútuo;
- Cumprimento de compromissos;
- Qualidade dos serviços;
- Conformidade legal e ética.

Não são admitidos acordos ou práticas que possam comprometer a imparcialidade, a reputação institucional ou a independência profissional.

19. Relacionamento com Órgãos Públicos

A atuação junto a órgãos públicos deve observar rigorosamente os princípios da Administração Pública e a legislação aplicável.

Todos os profissionais devem atuar de forma ética e transparente em qualquer interação com:

- Órgãos governamentais;
- Entidades da Administração Direta e Indireta;
- Empresas públicas;
- Autarquias;
- Fundações;
- Agentes públicos.

A organização não admite:

- Oferta de vantagens indevidas;
- Favorecimento pessoal;
- Intermediações inadequadas;
- Manipulação de informações;
- Fraudes em processos públicos;
- Influência indevida em decisões administrativas.

Todos os documentos, relatórios, pareceres e informações fornecidas a instituições públicas devem representar fielmente os fatos analisados.

20. Brindes, Presentes, Hospitalidades e Benefícios

A oferta ou recebimento de brindes, presentes, convites ou hospitalidades deve ser avaliada sob critérios de razoabilidade, transparência e finalidade legítima.

São permitidos apenas benefícios:

- De baixo valor;
- Compatíveis com práticas comerciais usuais;
- Que não influenciem decisões profissionais;

- Que não gerem expectativa de favorecimento.

São proibidos benefícios que possam:

- Comprometer a independência profissional;
- Influenciar decisões;
- Criar obrigação de reciprocidade;
- Ser interpretados como tentativa de obter vantagem indevida.

21. Uso Responsável de Recursos Tecnológicos

Os recursos tecnológicos utilizados para execução das atividades profissionais devem ser empregados de forma responsável, segura e exclusivamente para finalidades autorizadas.

São considerados recursos tecnológicos:

- Computadores;
- Dispositivos móveis;
- Sistemas corporativos;
- Plataformas de comunicação;
- Ambientes de armazenamento;
- Aplicações utilizadas nos projetos.

21.1 Responsabilidades dos Usuários

Os profissionais devem:

- Utilizar recursos tecnológicos conforme orientações institucionais;
- Proteger equipamentos e informações;
- Manter sistemas atualizados quando aplicável;
- Evitar instalação de softwares não autorizados;
- Utilizar recursos de comunicação de forma profissional;
- Adotar práticas seguras no acesso remoto.

21.2 Condutas Não Permitidas

Não é permitido:

- Compartilhar acessos individuais;
- Utilizar sistemas para atividades ilegais;
- Instalar softwares sem autorização;
- Armazenar informações confidenciais em locais inadequados;
- Burlar controles de segurança;
- Realizar qualquer ação que comprometa a disponibilidade, integridade ou confidencialidade das informações.

22. Gestão de Incidentes de Segurança e Privacidade

A organização mantém compromisso com a identificação, comunicação, tratamento e prevenção de incidentes relacionados à segurança da informação e proteção de dados.

São considerados incidentes:

- Acesso não autorizado a informações;
- Perda ou vazamento de dados;
- Roubo ou extravio de equipamentos;
- Compartilhamento indevido de documentos;
- Infecção por códigos maliciosos;
- Indisponibilidade de sistemas;
- Qualquer evento que comprometa informações protegidas.

22.1 Comunicação de Incidentes

Todos os profissionais devem comunicar imediatamente situações suspeitas ou confirmadas envolvendo:

- Vazamento de informações;
- Uso indevido de dados;

- Perda de dispositivos;
- Acessos não autorizados;
- Falhas de segurança.

A comunicação rápida permite a adoção de medidas preventivas, corretivas e de mitigação de impactos.

23. Relatórios Técnicos, Papéis de Trabalho e Produção Intelectual

Os relatórios, análises, diagnósticos, pareceres e demais documentos técnicos produzidos devem representar fielmente os trabalhos realizados.

Os profissionais devem assegurar:

- Clareza das informações apresentadas;
- Fundamentação técnica das conclusões;
- Registro adequado das evidências analisadas;
- Transparência quanto a limitações identificadas;
- Ausência de manipulação de resultados.

Os documentos produzidos representam patrimônio intelectual da organização e devem ser utilizados exclusivamente conforme finalidades autorizadas.

24. Canal de Ética e Comunicação de Condutas Inadequadas

A organização incentiva a comunicação responsável de situações que possam representar:

- Violação deste Código;
- Condutas antiéticas;
- Fraudes;
- Corrupção;
- Uso indevido de informações;
- Violações de segurança;
- Descumprimento de políticas internas.

As comunicações serão tratadas com confidencialidade, imparcialidade e respeito, buscando preservar os envolvidos e assegurar análise adequada dos fatos.

Sempre que possível, serão adotadas medidas para proteção contra qualquer forma de retaliação ao comunicante de boa-fé.

25. Responsabilidades pelo Cumprimento do Código

Todos os profissionais possuem responsabilidade individual pelo cumprimento deste Código.

São responsabilidades esperadas:

Profissionais e Colaboradores

- Conhecer e cumprir as diretrizes estabelecidas;
- Agir conforme princípios éticos;
- Proteger informações confidenciais;
- Comunicar situações inadequadas.

Lideranças

- Promover cultura de integridade;
- Orientar equipes;
- Dar exemplo de conduta ética;
- Garantir cumprimento das políticas institucionais.

Parceiros e Terceiros

- Respeitar princípios éticos equivalentes;
- Proteger informações acessadas;
- Cumprir obrigações contratuais e legais.

26. Treinamento e Conscientização

A organização incentiva a realização periódica de treinamentos relacionados a:

- Ética profissional;
- Segurança da Informação;

- Proteção de Dados;
- Compliance;
- Gestão de Riscos;
- Confidencialidade;
- Boas práticas profissionais.

O desenvolvimento contínuo de conhecimento é considerado elemento essencial para manutenção da qualidade e confiabilidade dos serviços prestados.

27. Descumprimento do Código

O descumprimento das disposições deste Código poderá resultar em medidas proporcionais à gravidade da situação, incluindo:

- Orientações formais;
- Advertências;
- Restrição de acessos;
- Encerramento de participação em projetos;
- Rescisão contratual;
- Comunicação às autoridades competentes, quando aplicável.

A aplicação de medidas observará critérios de proporcionalidade, análise dos fatos e respeito aos princípios de justiça e transparência.

28. Compromisso Institucional

A organização reafirma seu compromisso permanente com:

- Ética;
- Integridade;
- Confidencialidade;
- Segurança da Informação;
- Proteção de Dados;
- Independência profissional;

- Excelência técnica;
- Transparência;
- Responsabilidade corporativa.

A confiança estabelecida com clientes, empresas, órgãos públicos, parceiros e sociedade representa um valor essencial, que deve ser preservado por meio de atitudes responsáveis e profissionais.

Este Código representa o compromisso institucional de atuar de forma íntegra, segura e tecnicamente qualificada, contribuindo para organizações mais eficientes, transparentes e preparadas para os desafios do ambiente corporativo contemporâneo.

A ética orienta decisões.

A integridade fortalece relações.

A excelência técnica gera valor.