

AMARA TECH	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 1 de 15

AMARATECH

Programa de Integridade (LGPD e Compliance)

Histórico das Revisões

Revisão	Alterações	Responsável	Aprovador	Data	Assinatura do Aprovador
1.0	Emissão do Programa	Gabrielly Santos	Lucas Amorim	18/09/2026	LUCAS AMORIM ROSADO:38573955830 Assinado de forma digital por LUCAS AMORIM ROSADO:38573955830 Dados: 2026.09.28 18:09:57 -03'00'



Sumário

1. Glossário	5
2. Objetivo.....	5
3. Abrangência.....	6
4. Governança e Responsabilidades	6
4.1. Alta Administração	6
4.2. Compliance	6
4.3. Encarregado de Dados - DPO.....	7
4.4. Jurídico.....	7
4.5. Financeiro:	7
4.6 Recursos Humanos	7
4.7 Segurança da Informação e Tecnologia	7
4.8 Gestores e Lideranças.....	8
4.9 Colaboradores	8
4.10 Terceiros, Fornecedores e Parceiros	8
4.11 Responsabilidade Compartilhada	8
5. Princípios do Programa	9
6. Fundamentação Legal e Normativa	9
6.1. Lei Federal nº 12.846/2013	9
6.2 Decreto nº 12.304/2024	9
6.3 Portaria Normativa SE/CGU nº 226/2025	10
6.4 Pacto Brasil pela Integridade Empresarial	10
7. Código de Ética e Conduta	10
8. Prevenção à corrupção e a atos lesivos	10
9. Brindes, presentes, hospitalidades e benefícios	10
10. Conflito de Interesses.....	11
11. Gestão de Riscos de Integridade	11
12. Due Diligence de Terceiros	11
13. Controles contábeis e financeiros	11
14. Canais de Denúncia	12
14.1 Proteção contra retaliação.....	12
14.2 Apuração e investigação interna	12
15. Medidas Disciplinares.....	12
16. Treinamento e Comunicação	13
17. Integridade nas contratações e aquisições.....	13
18. Integração com LGPD e Segurança da Informação.....	13
19. Responsabilidade Social, Direitos Humanos e Sustentabilidade.....	13
20. Monitoramento do Programa.....	14

21. Indicadores de Integridade	14
22. Auditoria e Avaliação	14
23. Plano de Ação de Integridade	14
24. Pacto Brasil pela Integridade Empresarial	14
25. Documentação e Evidências	15
26. Melhoria Contínua	15
27. Disposições Finais.....	15
28. Aprovação e Vigência	15



	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 5 de 15

1. Glossário

Compliance: conjunto de mecanismos, procedimentos e controles destinados a assegurar o cumprimento das leis, regulamentos, normas e políticas internas aplicáveis à organização.

Integridade: conjunto de princípios e práticas voltados à prevenção, detecção e tratamento de irregularidades, fraudes, corrupção e desvios de conduta.

Programa de Integridade: conjunto estruturado de mecanismos e procedimentos internos destinados à prevenção, detecção e correção de atos ilícitos e demais condutas inadequadas.

Risco de Integridade: possibilidade de ocorrência de fraude, corrupção, conflito de interesses, irregularidade ou outra conduta que possa comprometer a organização.

Due Diligence: processo de análise e verificação de informações de terceiros, fornecedores, parceiros ou demais partes relacionadas, com o objetivo de identificar riscos.

Conflito de Interesses: situação em que interesses pessoais ou particulares possam interferir, ou aparentar interferir, no exercício imparcial das atividades profissionais.

Canal de Denúncias: meio disponibilizado pela organização para recebimento de relatos sobre possíveis irregularidades, violações de normas ou condutas inadequadas.

Agente Público: pessoa que exerce, ainda que temporariamente ou sem remuneração, função pública, cargo, emprego ou atividade em órgão ou entidade da Administração Pública.

Atos Lesivos: condutas praticadas por pessoa jurídica que atentem contra o patrimônio público, princípios da Administração Pública ou compromissos internacionais assumidos pelo Brasil, conforme a Lei nº 12.846/2013.

Terceiro: pessoa física ou jurídica que mantenha relação comercial, contratual ou profissional com a Amaratech.

2. Objetivo

O Programa de Integridade Empresarial da Amaratech Cybersecurity estabelece princípios, diretrizes, mecanismos e procedimentos destinados à prevenção, detecção e tratamento de atos de corrupção, fraude, irregularidades, conflitos de interesses e demais condutas incompatíveis com os valores e compromissos da organização.

O Programa tem como finalidade fortalecer uma cultura organizacional baseada em ética, integridade, transparência, responsabilidade, respeito às pessoas, conformidade e prevenção de riscos, abrangendo as relações da Amaratech com colaboradores, clientes,

	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 6 de 15

fornecedores, parceiros comerciais, agentes públicos e demais partes interessadas. Busca também estabelecer mecanismos capazes de demonstrar a efetividade das medidas adotadas pela organização, considerando os parâmetros previstos na legislação e nas orientações da Controladoria Geral da União.

O Decreto nº 12.304/2024 define programa de integridade como o conjunto de mecanismos e procedimentos internos de integridade, auditoria, incentivo à denúncia e aplicação efetiva de códigos de ética, conduta e políticas de prevenção à corrupção, com objetivos de prevenir, detectar e sanar desvios, fraudes, irregularidades e atos lesivos, mitigar riscos sociais e ambientais e fomentar uma cultura de integridade.

3. Abrangência

O Programa de Integridade aplica-se à Amaratech Cybersecurity e deverá orientar a atuação de seus administradores, gestores, empregados, estagiários, prestadores de serviços, representantes, consultores, parceiros comerciais e demais terceiros que atuem em nome ou em benefício da organização.

Todos os profissionais vinculados à empresa deverão observar os princípios e diretrizes estabelecidos pelo Programa, independentemente de cargo, função, nível hierárquico, modalidade de contratação ou local de atuação. Os terceiros que mantenham relacionamento comercial ou institucional com a Amaratech poderão ser submetidos a procedimentos de avaliação de integridade proporcionais ao nível de risco identificado na relação.

4. Governança e Responsabilidades

A governança do Programa de Integridade da Amaratech Cybersecurity será realizada de forma integrada, considerando a participação da Alta Administração, da área de Compliance, do Encarregado pelo Tratamento de Dados Pessoais, das áreas de Recursos Humanos, Jurídico, Financeiro, Tecnologia e Segurança da Informação, dos gestores e dos demais colaboradores e terceiros, de acordo com suas respectivas atribuições.

4.1. Alta Administração

Compete à Alta Administração demonstrar compromisso permanente com o Programa de Integridade, promovendo sua implementação, manutenção e aprimoramento. Caberá à Diretoria aprovar as principais políticas e diretrizes relacionadas à integridade, disponibilizar recursos compatíveis com as necessidades do Programa, acompanhar os principais riscos identificados e assegurar que medidas adequadas sejam adotadas diante de eventuais irregularidades.

A Alta Administração deverá também promover uma cultura organizacional baseada na ética, transparência, responsabilidade e conformidade, assegurando que os princípios de integridade sejam considerados nas decisões estratégicas e na condução das atividades empresariais.

4.2. Compliance

Compete à área de Compliance coordenar e apoiar a implementação, manutenção, monitoramento e aprimoramento do Programa de Integridade. Caberá à área acompanhar os riscos de integridade, propor políticas e procedimentos, orientar colaboradores e

	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 7 de 15

gestores, apoiar processos de Due Diligence, acompanhar denúncias e situações de potencial irregularidade e promover ações de conscientização e treinamento.

A área de Compliance deverá manter registros e evidências relacionados às atividades do Programa, acompanhar planos de ação, apoiar avaliações internas e externas e reportar à Alta Administração informações relevantes sobre o funcionamento do Programa e sobre situações que possam representar riscos significativos à organização.

4.3. Encarregado de Dados - DPO

Compete ao Encarregado pelo Tratamento de Dados Pessoais, no âmbito de suas atribuições, apoiar a integração entre o Programa de Integridade e as práticas de privacidade e proteção de dados pessoais.

O DPO deverá orientar quanto ao tratamento adequado de dados pessoais em processos relacionados a denúncias, investigações, Due Diligence, controles internos, monitoramentos e demais atividades do Programa, contribuindo para que sejam observados os princípios e requisitos estabelecidos pela legislação de proteção de dados pessoais.

4.4. Jurídico

Compete à área Jurídica prestar suporte técnico-jurídico na interpretação e aplicação da legislação relacionada ao Programa de Integridade, apoiando a elaboração e revisão de políticas, contratos, cláusulas de integridade e demais instrumentos jurídicos. A área Jurídica poderá também apoiar análises de riscos legais, investigações internas, medidas disciplinares, relações com órgãos públicos e demais situações que demandem avaliação jurídica especializada.

4.5. Financeiro:

Compete à área Financeira assegurar que os processos financeiros e contábeis observem os controles internos estabelecidos pela organização, mantendo registros adequados, completos e rastreáveis das operações realizadas. A área deverá apoiar a prevenção de pagamentos indevidos, despesas sem documentação adequada, movimentações incompatíveis com os procedimentos internos e demais situações que possam representar riscos financeiros ou de integridade.

4.6 Recursos Humanos

Compete à área de Recursos Humanos apoiar a disseminação da cultura de integridade entre os colaboradores, incluindo a integração de novos profissionais, comunicação de políticas internas, realização e controle de treinamentos e apoio aos procedimentos relacionados a medidas disciplinares. A área deverá atuar em conjunto com Compliance na identificação de necessidades de capacitação e na promoção de ambiente profissional pautado pelo respeito, ética, diversidade, não discriminação e prevenção de situações de assédio ou outras condutas inadequadas.

4.7 Segurança da Informação e Tecnologia

Compete às áreas de Tecnologia e Segurança da Informação apoiar a proteção dos sistemas, informações e recursos tecnológicos utilizados na execução do Programa de Integridade. Essas áreas deverão contribuir para a implementação de controles de acesso, proteção de informações, preservação de evidências digitais, segurança dos registros e

	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 8 de 15

prevenção de acessos ou tratamentos não autorizados, observando as políticas internas de Segurança da Informação e proteção de dados pessoais.

4.8 Gestores e Lideranças

Compete aos gestores e líderes assegurar que suas respectivas equipes conheçam e cumpram as políticas, procedimentos e diretrizes de integridade aplicáveis às suas atividades. Os gestores deverão atuar como referência de conduta ética, comunicar situações de risco ou irregularidades identificadas e colaborar com Compliance e demais áreas responsáveis na implementação de medidas preventivas e corretivas.

Também deverão evitar qualquer prática que possa caracterizar favorecimento, conflito de interesses, retaliação ou tratamento inadequado aos colaboradores que realizem comunicações ou denúncias de boa-fé.

4.9 Colaboradores

Compete a todos os colaboradores conhecer e cumprir as disposições deste Programa, do Código de Ética e Conduta e das demais políticas e procedimentos internos aplicáveis às suas atividades.

Os colaboradores deverão atuar de maneira ética, transparente e responsável, utilizar adequadamente os recursos da organização, preservar informações corporativas e comunicar situações que possam representar fraude, corrupção, conflito de interesses, violação de políticas ou qualquer outra irregularidade. A responsabilidade individual pela integridade deverá ser observada independentemente da posição hierárquica ou função exercida na organização.

4.10 Terceiros, Fornecedores e Parceiros

Os terceiros, fornecedores, prestadores de serviços e parceiros que mantenham relacionamento com a Amaratech, deverão observar as normas legais aplicáveis e, quando previsto contratualmente, as diretrizes de integridade estabelecidas pela organização. Os terceiros deverão fornecer informações verdadeiras e suficientes para os procedimentos de avaliação de integridade aplicáveis, comunicar potenciais conflitos de interesses e abster-se de praticar atos que possam comprometer a integridade da Amaratech Cybersecurity.

Quando identificados riscos relevantes, a organização poderá estabelecer medidas adicionais de controle, acompanhamento ou mitigação, inclusive mediante cláusulas contratuais específicas.

4.11 Responsabilidade Compartilhada

A efetividade do Programa de Integridade depende da atuação conjunta de todas as áreas e pessoas que integram ou se relacionam com a Amaratech Cybersecurity. Dessa forma, nenhuma área ou função deverá ser considerada isoladamente responsável pela integridade da organização.

A responsabilidade compartilhada deverá ocorrer de maneira proporcional às atribuições, ao nível de autoridade e aos riscos relacionados a cada função, preservando-se a independência necessária para avaliação, monitoramento e tratamento de situações que possam comprometer a integridade empresarial.

5. Princípios do Programa

I – Integridade

Atuação ética, responsável e coerente com as normas legais e internas;

II – Transparência

Disponibilização de informações adequadas, verdadeiras e necessárias às partes interessadas;

III – Ética

Tomada de decisões baseada em princípios éticos e profissionais;

IV – Prevenção

Atuação antecipada para identificação e mitigação de riscos;

V – Responsabilização

Definição clara de responsabilidades e consequências pelo descumprimento das normas;

VI – Independência

Atuação técnica e imparcial das funções responsáveis pelo Programa, dentro das estruturas organizacionais disponíveis;

VII – Melhoria contínua

Avaliação periódica e aperfeiçoamento permanente dos mecanismos de integridade.

6. Fundamentação Legal e Normativa

O Programa será estruturado considerando, principalmente:

6.1. Lei Federal nº 12.846/2013

A Lei Anticorrupção estabelece a responsabilização objetiva administrativa e civil das pessoas jurídicas pela prática de atos lesivos contra a Administração Pública, nacional ou estrangeira. A legislação constitui referência central para a criação de mecanismos preventivos, controles internos e práticas de integridade empresarial.

6.2 Decreto nº 12.304/2024

O Decreto estabelece parâmetros para Programas de Integridade e sua avaliação em determinadas hipóteses relacionadas à Lei nº 14.133/2021. Entre os parâmetros estão comprometimento da alta gestão, padrões de conduta, políticas de integridade, extensão das regras a terceiros, treinamentos, gestão de riscos, registros contábeis, controles internos e mecanismos específicos relacionados às interações com o setor público.

6.3 Portaria Normativa SE/CGU nº 226/2025

A Portaria estabelece procedimentos e metodologia para avaliação dos programas de integridade previstos no Decreto nº 12.304/2024. A metodologia considera aspectos relacionados à implantação, desenvolvimento e aperfeiçoamento do Programa de Integridade.

6.4 Pacto Brasil pela Integridade Empresarial

O Programa também adota como referência os compromissos e diretrizes do Pacto Brasil pela Integridade Empresarial, iniciativa voluntária da CGU destinada a estimular empresas e entidades privadas a assumirem compromisso público com a integridade e a adotarem ações concretas para sua implementação.

A adesão ao Pacto envolve a assinatura do Termo de Adesão e a realização da autoavaliação disponibilizada pela CGU, sendo estabelecido prazo de até 180 dias para conclusão da autoavaliação após a adesão.

7. Código de Ética e Conduta

A Amaratech Cybersecurity deverá manter Código de Ética e Conduta compatível com os princípios deste Programa, estabelecendo padrões esperados de comportamento profissional e diretrizes relacionadas à integridade, respeito, transparência, relacionamento com terceiros, conflito de interesses, presentes, brindes, hospitalidades, proteção de informações e comunicação de irregularidades.

O Código deverá ser divulgado aos colaboradores e, quando aplicável, aos terceiros que mantenham relacionamento com a organização. Sua observância constitui elemento fundamental para o desenvolvimento e manutenção da cultura de integridade empresarial.

8. Prevenção à corrupção e a atos lesivos

A Amaratech Cybersecurity não admite a prática de corrupção, suborno, fraude ou qualquer conduta destinada à obtenção de vantagem indevida para a organização, seus colaboradores ou terceiros.

É proibido oferecer, prometer, autorizar, conceder, solicitar ou receber vantagem indevida com a finalidade de influenciar decisões, obter benefícios comerciais, direcionar contratações, acelerar procedimentos ou alcançar resultado incompatível com a legislação. Todas as relações comerciais e institucionais deverão ser conduzidas de maneira legítima, transparente e documentada, especialmente quando envolverem agentes públicos ou entidades da Administração Pública.

9. Brindes, presentes, hospitalidades e benefícios

A oferta ou recebimento de brindes, presentes, hospitalidades, convites ou benefícios deverá observar critérios de razoabilidade, transparência e finalidade legítima, sendo vedadas situações capazes de caracterizar vantagem indevida ou comprometer a independência das decisões profissionais. Nas relações com agentes públicos deverão ser observadas as restrições previstas na legislação e nas normas aplicáveis. Situações que possam gerar dúvida deverão ser previamente submetidas à área de Compliance ou à autoridade interna competente.

AMARA TECH	Programa de Integridade		ORIGINAL Pública
	Emissão: 18/09/2026	Próxima Revisão: 18/09/2027	Página 11 de 15

10. Conflito de Interesses

Os colaboradores deverão evitar situações em que interesses pessoais, familiares, financeiros ou profissionais possam interferir ou aparentar interferir na tomada de decisões relacionadas às atividades da Amaratech Cybersecurity. As situações de potencial conflito deverão ser comunicadas de forma transparente para avaliação e adoção das medidas necessárias. A identificação de um conflito não significa necessariamente a existência de irregularidade, mas exige tratamento adequado para preservar a imparcialidade e a integridade das decisões.

11. Gestão de Riscos de Integridade

A gestão dos riscos de integridade deverá ocorrer de forma contínua e integrada à gestão de riscos corporativos da organização, considerando as características das atividades, processos, relacionamentos e operações da Amaratech Cybersecurity.

Os riscos poderão estar relacionados à corrupção, fraude, conflito de interesses, contratações, terceiros, relacionamento com agentes públicos, informações financeiras, segurança da informação, proteção de dados, processos internos e reputação. A identificação dos riscos deverá ser acompanhada de avaliação de probabilidade e impacto, permitindo a definição de controles e medidas preventivas ou corretivas proporcionais ao nível de exposição identificado.

12. Due Diligence de Terceiros

A Amaratech Cybersecurity poderá realizar procedimentos de Due Diligence previamente ao estabelecimento ou à continuidade de determinadas relações comerciais, considerando o nível de risco associado ao terceiro. A avaliação poderá considerar informações cadastrais, societárias, reputacionais, histórico de relacionamento com o Poder Público, existência de sanções e outras informações relevantes para a análise de integridade. A profundidade da avaliação deverá ser proporcional ao risco identificado e à natureza da relação estabelecida.

13. Controles contábeis e financeiros

A organização deverá manter controles financeiros e contábeis destinados a assegurar o adequado registro, documentação e rastreabilidade das operações realizadas. As transações deverão ser registradas de maneira completa, precisa e tempestiva, sendo proibida a criação ou manutenção de registros falsos, incompletos ou destinados a ocultar pagamentos ou benefícios indevidos. Pagamentos, reembolsos, contratações e demais movimentações financeiras deverão observar os procedimentos internos e possuir documentação compatível com sua natureza.

14. Canais de Denúncia

Todo o público de relacionamento da Amaratech tem os seguintes Canais de Denúncia para comunicar casos de violação ou suspeita de violação a quaisquer regras previstas no Código de Ética e Conduta, na legislação e nas políticas e procedimentos internos da Empresa. O tratamento deverá observar:

Recebimento → Registro → Triagem → Classificação → Investigação → Conclusão → Medidas corretivas → Encerramento.

Canal de Denúncias: <https://privacidade.amaratech.com.br/>
E-mail de Compliance: compliance@amaratech.com.br

Os Canais de Denúncia garantem total confidencialidade, sigilo e anonimato do denunciante de boa-fé na comunicação de quaisquer violações.

14.1 Proteção contra retaliação

A Amaratech Cybersecurity não tolerará retaliações contra pessoas que, de boa-fé, realizem denúncias, comuniquem irregularidades, cooperem com investigações ou solicitem orientação relacionada ao cumprimento das normas de integridade. Alegações de retaliação deverão ser avaliadas adequadamente e poderão resultar na adoção das medidas administrativas cabíveis. A proteção contra retaliação não impede a responsabilização de pessoas que deliberadamente apresentem denúncias falsas com finalidade de prejudicar terceiros.

14.2 Apuração e investigação interna

As suspeitas de irregularidades deverão ser submetidas a análise e, quando necessário, investigação interna compatível com sua natureza e gravidade.

As apurações deverão observar imparcialidade, confidencialidade, documentação, preservação de evidências, respeito aos envolvidos e legislação aplicável. Quando necessário, poderão ser envolvidos profissionais de diferentes áreas ou especialistas externos para apoio técnico, jurídico, financeiro, contábil, tecnológico ou investigativo.

15. Medidas Disciplinares

O descumprimento das políticas poderá resultar em medidas disciplinares proporcionais à gravidade da conduta, observadas a legislação aplicável e as normas internas.

Medidas	
orientação	bloqueio de acesso
advertência	descredenciamento
suspensão	medidas judiciais cabíveis
desligamento	medidas administrativas cabíveis
rescisão contratual	

16. Treinamento e Comunicação

A Amaratech Cybersecurity deverá promover ações periódicas de treinamento e conscientização relacionadas à ética, integridade, prevenção à corrupção, conflitos de interesses, relacionamento com agentes públicos, proteção de informações, proteção de dados pessoais e demais temas relacionados aos riscos identificados. Os treinamentos deverão considerar as responsabilidades e os riscos associados às diferentes funções e públicos internos.

As ações de comunicação deverão reforçar os valores e compromissos do Programa e contribuir para a consolidação de uma cultura organizacional baseada na ética e na conformidade.

17. Integridade nas contratações e aquisições

Os processos de contratação de fornecedores, parceiros e prestadores de serviços deverão observar critérios objetivos, transparentes e compatíveis com os procedimentos internos da organização. Sempre que aplicável, deverão ser considerados aspectos relacionados à integridade, reputação, capacidade técnica, regularidade documental e riscos associados ao terceiro.

Os instrumentos contratuais poderão estabelecer cláusulas específicas relacionadas ao cumprimento da legislação anticorrupção, ética, confidencialidade, proteção de dados e Segurança da Informação.

18. Integração com LGPD e Segurança da Informação

O Programa de Integridade deverá atuar de maneira integrada às práticas de privacidade, proteção de dados pessoais e Segurança da Informação da Amaratech Cybersecurity. O tratamento de informações decorrente de denúncias, investigações, Due Diligence, controles internos e processos de integridade deverá observar os princípios e requisitos da legislação de proteção de dados pessoais, especialmente quanto à finalidade, necessidade, segurança, confidencialidade e controle de acesso.

A organização deverá adotar medidas técnicas e administrativas apropriadas para proteger as informações relacionadas ao Programa contra acesso não autorizado, perda, alteração, divulgação indevida ou qualquer outra forma de tratamento inadequado.

19. Responsabilidade Social, Direitos Humanos e Sustentabilidade

A Amaratech Cybersecurity reconhece a importância da condução responsável de suas atividades e deverá buscar a observância dos direitos humanos, da dignidade das pessoas, da igualdade de tratamento e da não discriminação.

As relações com colaboradores, fornecedores, clientes e demais partes interessadas deverão ser conduzidas de forma ética e responsável, considerando riscos relacionados a trabalho infantil, trabalho análogo à escravidão, assédio, discriminação e demais práticas incompatíveis com os princípios da organização.

20. Monitoramento do Programa

O Programa de Integridade deverá ser monitorado periodicamente para verificar sua implementação, funcionamento e aderência às necessidades da organização. O monitoramento poderá considerar informações provenientes de treinamentos, denúncias, investigações, Due Diligence, avaliações de riscos, auditorias, controles internos, indicadores, não conformidades e demais fontes relevantes. Os resultados deverão subsidiar ações corretivas e preventivas e contribuir para o aprimoramento contínuo do Programa.

21. Indicadores de Integridade

A Amaratech Cybersecurity poderá estabelecer indicadores destinados a acompanhar o funcionamento e a evolução do Programa de Integridade. Os indicadores poderão considerar a realização de treinamentos, quantidade e natureza das manifestações recebidas, tratamento das denúncias, realização de avaliações de terceiros, identificação de conflitos de interesses, resultados de auditorias e implementação de medidas corretivas. Os indicadores deverão ser analisados de maneira contextualizada e utilizados como instrumentos de acompanhamento, gestão e melhoria contínua.

22. Auditoria e Avaliação

O Programa de Integridade poderá ser submetido a avaliações internas ou externas, conforme as necessidades da organização e os riscos identificados. As avaliações deverão verificar a existência, implementação e efetividade dos mecanismos previstos neste Programa, permitindo identificar deficiências, oportunidades de melhoria e necessidades de atualização.

Os resultados das avaliações deverão ser documentados e, quando necessário, acompanhados de planos de ação com responsáveis e prazos definidos.

23. Plano de Ação de Integridade

Com base nos resultados das avaliações de riscos, auditorias, investigações e monitoramentos, a Amaratech Cybersecurity poderá estabelecer Plano de Ação de Integridade destinado à implementação de medidas preventivas, corretivas ou de mitigação dos riscos identificados. As ações estabelecidas deverão possuir responsáveis, prazos, critérios de acompanhamento e evidências de implementação, permitindo verificar sua execução e efetividade.

O Plano de Ação deverá ser revisado periodicamente e atualizado sempre que houver alteração relevante nos riscos ou processos da organização.

24. Pacto Brasil pela Integridade Empresarial

A Amaratech Cybersecurity poderá utilizar as diretrizes e compromissos relacionados ao Pacto Brasil pela Integridade Empresarial como referência para o fortalecimento de sua cultura de integridade e para o aprimoramento de suas práticas de prevenção e combate à corrupção. Eventual adesão ou participação em iniciativas relacionadas ao Pacto deverá ser acompanhada de medidas concretas de implementação, monitoramento e demonstração dos compromissos assumidos pela organização.

25. Documentação e Evidências

A organização deverá manter documentação suficiente para demonstrar a implementação e o funcionamento dos mecanismos de integridade, observados os requisitos legais de guarda, confidencialidade, segurança e proteção de dados pessoais. Poderão constituir evidências do Programa as políticas internas, Código de Ética e Conduta, registros de treinamentos, avaliações de riscos, procedimentos de Due Diligence, registros de denúncias, relatórios de investigação, controles financeiros, contratos, planos de ação, atas, comunicações internas, avaliações e relatórios de monitoramento.

A documentação deverá ser armazenada de maneira segura e acessível somente às pessoas autorizadas, respeitando os períodos de retenção estabelecidos pela organização e pela legislação aplicável.

26. Melhoria Contínua

O Programa de Integridade deverá ser continuamente aprimorado com base nos resultados obtidos, nas alterações legislativas e regulatórias, nos riscos identificados, nas experiências decorrentes de incidentes e investigações, nas avaliações internas e externas e nas necessidades estratégicas da organização.

A melhoria contínua deverá considerar tanto a implementação de novos controles quanto a revisão daqueles que apresentem baixa efetividade, sobreposição, inadequação ou incompatibilidade com os processos atuais da empresa.

27. Disposições Finais

O Programa de Integridade deverá ser interpretado conjuntamente com o Código de Ética e Conduta, as políticas internas, os procedimentos corporativos, as normas de Segurança da Informação, os documentos relacionados à privacidade e proteção de dados pessoais e demais instrumentos internos aplicáveis.

Todos os integrantes da organização possuem responsabilidade pela observância das disposições estabelecidas neste Programa e pela promoção de ambiente profissional pautado pela ética, transparência, respeito e conformidade. As situações não previstas neste documento deverão ser analisadas pela área competente, considerando a legislação aplicável, os princípios de integridade e os interesses legítimos da organização.

O Programa deverá ser revisado periodicamente ou sempre que houver alteração relevante na legislação, na estrutura organizacional, nos processos internos, no perfil de riscos ou nas atividades desenvolvidas pela Amaratech Cybersecurity.

28. Aprovação e Vigência

Este Programa de Integridade entra em vigor na data de sua aprovação e deverá ser amplamente divulgada a todos os envolvidos.